



Powerful, Robust Anti-malware Protection for Medium- to Large-sized Businesses

- High-performance, high-value Next Generation Firewall (NGFW) for medium and large-sized businesses and campuses
- Anti-malware protection with firewall, anti-virus, anti-spam, content filtering, IDP, next-generation application intelligence and SSL inspection
- Robust SSL, IPSec and L2TP over IPSec VPN connectivity and VPN High Availability (HA)
- Unified security policy streamlines the configuration and management efforts
- Built-in WLAN controller for centralized AP management and effortless WLAN scalability of up to 66 APs
- ZyXEL One Network is supported
- The brand-new firmware update — ZLD4.20 — supports Cloud Helper, PCI DSS compliance, Hotspot Management and Device HA Pro

As a business grows, so does the scope of its network. New users and devices connect at an ever-increasing rate. Add to this an array of applications, like cloud-based services, and one begins to understand the challenge facing today's enterprises. It's a continuous cycle — demand for high network availability increases alongside the need for more Internet access, not to mention additional user controls and improved security measures.

The new ZyXEL USG Extreme Series is a line of next-generation firewalls (NGFW) designed to meet this challenge head-on with high availability, anti-malware protection, access management, and consolidated policy enforcement for medium- to large-sized businesses and campuses. The ZyXEL USG Extreme Series provides WAN and VPN load balancing, failover to ensure nonstop business communications, and our Hotspot Management solution for secure network connectivity with easy access.



Benefits

Powerful, Robust and Always-Online

ZyXEL USG Extreme Series delivers high-access quality to help businesses satisfy the demand for always-online communications. For internal deployments, the USG Extreme Series provides active-passive High-Availability (HA) service to support device or connection failover. With Device HA Pro service, the USG Extreme Series also supports instant failover, so connections are always maintained when a failover event occurs. For external deployments, the USG Extreme Series features multi-WAN load balancing/failover and a comprehensive mobile broadband USB modem support list for WAN backup operations. The Extreme Series also supports IPSec load balancing and failover, providing additional resilience for mission-critical VPN failover with VTI Interface deployments.

Impregnable Protection and Optimization

ZyXEL USG Extreme Series thoroughly protects networks with industry-leading firewall, Anti-Malware/Virus, Anti-spam, Content Filtering, IDP, and Application Intelligence functionality. Regulate unauthorized use of Web applications over your network, such as Facebook, Google apps, and Netflix, among others. ZyXEL security measures are enhanced with SSL Inspection, blocking threats hidden in SSL-encrypted connections while facilitating deeper policy enforcement. Furthermore, newly improved Content Filtering 2.0 enhances HTTPS Domain Filter, Browser SafeSearch, and Geo IP Blocking for an array of security enhancements to ensure clean Web connections.



ZyXEL onenetwork
Redefining network integration

USG1900/1100
Unified Security Gateway—
Extreme Series



Best TCO for Access Expansion

People expect network access regardless of time or location. As a result, hotspots are in demand in an ever-expanding assortment of locations. The ZyXEL USG Extreme Series integrated with ZyXEL AP Controller technology enables users to manage up to 66 APs from a centralized user interface. In addition, ZyXEL Hotspot Management delivers a unified solution for business networks with user-friendly tools like Billing System, Walled Garden, Multiple Authentication, 3rd Party Social Login and User Agreement. With ZyXEL USG Extreme Series, businesses can now deploy or expand a managed Wi-Fi network with minimal effort.

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. The ZyXEL 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.

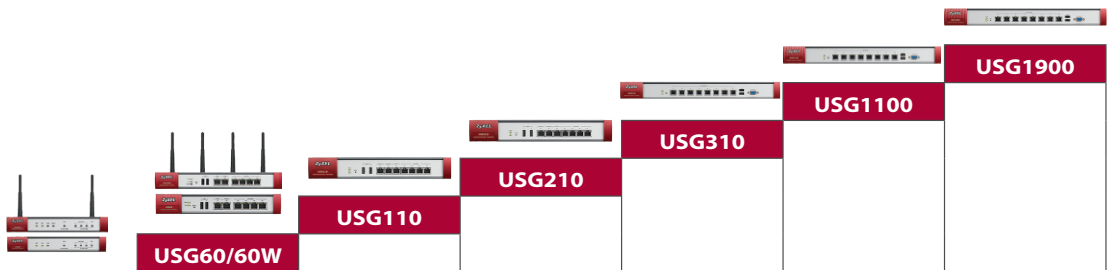
ZyXEL One Network experience

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 Wi-Fi AP and to Gateway.

Stay Secure and Up-to-Date with OneSecurity.com

ZyXEL provides frequent and timely updates in response to the latest security threats and advisories through OneSecurity.com — our free online service portal. OneSecurity.com offers informative network security resources and the know-how to assist businesses and IT administrators in keeping their network operations safe in the digital age. Information and resources can be found with one click via the GUI of ZyXEL USG Extreme and ZyWALL series products. IT staff can quickly and easily catch up on the latest threats, and then proceed to walkthroughs and troubleshooting protocols with the help of easy-to-follow FAQs — all provided to help users secure their networks and simplify management of our UTM products.

Next-Gen USG Quick Finder



Model	USG40/40W	USG60/60W	USG110	USG210	USG310	USG1100	USG1900
Description	Performance Series		Advanced Series			Extreme Series	
Multi-WAN	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Unified security policy	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SSL inspection	-	-	Yes	Yes	Yes	Yes	Yes
Link Aggregation (LAG)	-	-	-	-	Yes	Yes	Yes
Port grouping	Yes	Yes	Yes	Yes	-	-	-
Device HA	-	-	Yes	Yes	Yes	Yes	Yes
Device HA Pro	-	-	Yes	Yes	Yes	Yes	Yes
Easy Mode	Yes	Yes	-	-	-	-	-
Cloud Helper	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PCI DSS Compliance	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Content Filtering 2.0*	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hotspot Management	-	-	-	-	Yes	Yes	Yes

* SSL Inspection must be enabled for Content Filtering 2.0 Safe Search to function properly.

License Features



Anti-Virus



Anti-Spam



Intrusion
Detection &
Prevention



Application
Intelligence



Content Filtering
2.0



Hotspot
Management



HA Pro

The ZyXEL USG Extreme Series 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.

Feature Highlights



Multiple
WANs

Multi-WAN & Mobile Broadband

The ZyXEL USG Extreme Series provides non-stop Internet uptime with multi-WAN and mobile broadband support. Multi-WAN works with two or more Ethernet WAN connections for active-active WAN load balancing or active-passive failover. Comprehensive mobile broadband USB modems are also supported for WAN backup.



Unified Security
Policy

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

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.



ZON Utility

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 Wi-Fi APs, switches and gateways.



SSL Inspection

SSL Inspection

SSL inspection enables the ZyXEL Extreme Series to provide not only comprehensive security, but also deeper policy enforcement. It enables the USG's application intelligence, IDP, content filtering and anti-virus to inspect traffic in SSL encrypted connections and block threats that usually go unseen.



VPN

Robust VPN

ZyXEL USGs 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 cryptographic, the ZyXEL USGs provide the most secure Policy-based and route-based VPN for business communications.



Integrated WLAN
Controller

Integrated WLAN Controller

The integrated WLAN controller supports CAPWAP, and enables centralized authentication and access management of multiple APs in the network. The ZyXEL USG Extreme Series can manage 2 APs by default, and up to 66 APs with license upgrade.



PCI DSS
Compliance

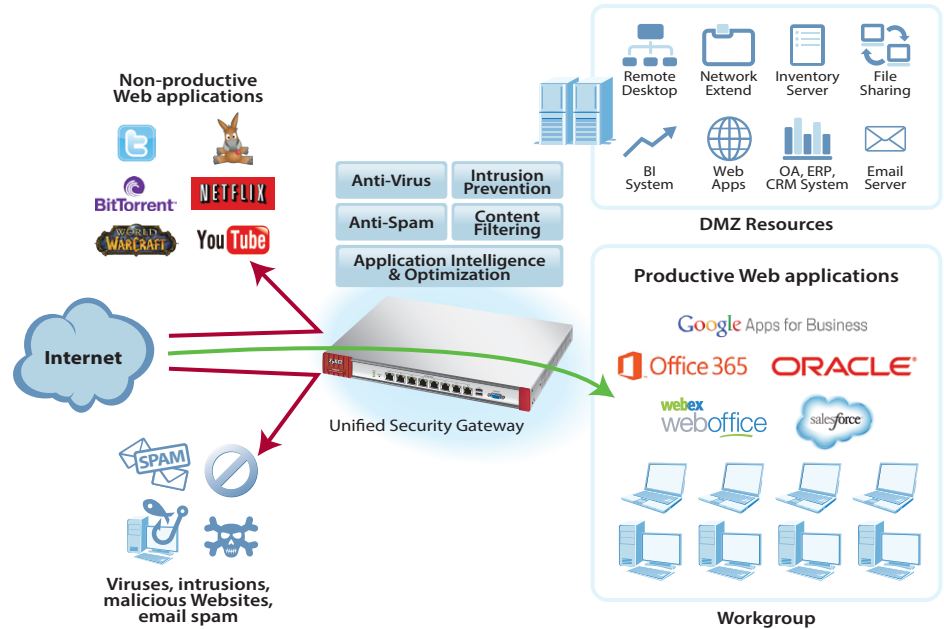
PCI-DSS Compliance

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 DSS 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.

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 enables businesses to deny access to Websites that are malicious or not business-related
- Application intelligence technology not only enable businesses to block or throttle non-productive Web applications, but also optimize Web applications that increase productivity

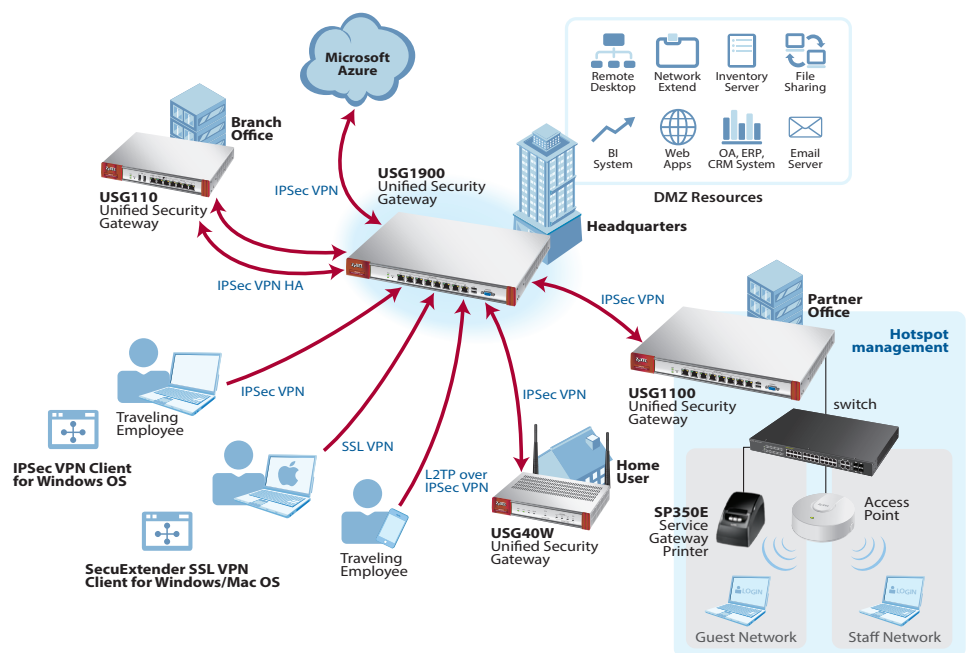


VPN application



- Branch offices, partners and home users can deploy ZyXEL USGs/ ZyWALLs 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 USG/ZyWALL can also establish an IPSec VPN connection with Microsoft Azure for secured access to a variety of cloud-based applications

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)



Specifications

Model		Extreme Series	
		USG1900	USG1100
Product photo			
Hardware Specifications			
10/100/1000 Mbps RJ-45 ports		8 (configurable)	8 (configurable)
USB ports		2	2
Console port		Yes (DB9)	Yes (DB9)
Rack-mountable		Yes	Yes
System Capacity & Performance ^{*1}			
SPI firewall throughput (Mbps) ^{*2}		7,000	6,000
VPN throughput (Mbps) ^{*3}		900	800
IDP throughput (Mbps) ^{*4}		650	550
AV throughput (Mbps) ^{*4}		600	500
UTM throughput (AV and IDP) ^{*4}		600	500
Concurrent devices (default/max.)		1500/2000	800/1500
Max. TCP concurrent sessions ^{*5}		500,000	500,000
Max. concurrent IPsec VPN tunnels ^{*6}		2,000	1,000
Concurrent SSL VPN user no. (default/max.)		250/750	250/500
Customizable zones		Yes	Yes
IPv6 support		Yes	Yes
VLAN interface		128	128
WLAN Management			
AP Controller (APC) support		Yes	Yes
Managed AP number (default/max.)		2/66	2/66
Key Software Features			
Firewall		Yes	Yes
Virtual private network (VPN)		Yes (IPSec, SSL, L2TP over IPSec)	Yes (IPSec, SSL, L2TP over IPSec)
Bandwidth Management		Yes	Yes
Logging and Monitoring		Yes	Yes
SSL (HTTPS) inspection		Yes	Yes
Unified security policy		Yes	Yes
Cloud Helper		Yes	Yes
HA		Yes	Yes
License Service			
Anti-virus (AV)		Yes	Yes
Intrusion detection and prevention (IDP) & Application Intelligence		Yes	Yes
Anti-spam		Yes	Yes
Content filtering (CF2.0) ^{*7}		Yes	Yes
Device HA Pro		Yes	Yes
Hostpot Management		Yes	Yes
Power Requirements			
Power input		100 - 240 V AC, 50/60 Hz, 1.3 A max.	100 - 240 V AC, 50/60 Hz, 1.3 A max.
Max. power consumption (watt)		58.5	58.5
Heat dissipation (BTU/hr)		199.61	199.61
Physical Specifications			
Item	Dimensions (WxDxH)(mm/in.)	430 x 250 x 44/16.93 x 9.84 x 1.73	430 x 250 x 44/16.93 x 9.84 x 1.73
	Weight (kg/lb.)	3.3/7.28	3.3/7.28
Packing	Dimensions (WxDxH)(mm/in.)	519 x 392 x 163/20.43 x 15.43 x 6.42	519 x 392 x 163/20.43 x 15.43 x 6.42
	Weight (kg/lb.)	4.8/10.58	4.8/10.58
Included accessories		• Power cord • Rack mounting kit	• Power cord • Rack mounting kit
Environmental Specifications			
Operating	Temperature	0°C to 40°C (32°F to 104°F)	0°C to 40°C (32°F to 104°F)
	Humidify	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)
	Humidify	10% to 90% (non-condensing)	10% to 90% (non-condensing)
MTBF (hr)		560,811.5	560,811.5

Model	USG1900	USG1100
Certifications		
EMC	FCC Part 15 (Class A), CE EMC (Class A), C-Tick (Class A), BSMI	FCC Part 15 (Class A), CE EMC (Class A), C-Tick (Class A), BSMI
Safety	LVD (EN60950-1), BSMI	LVD (EN60950-1), BSMI

Note:

* This matrix with firmware ZLD 4.20 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 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: SafeSearch function in CF2.0 need to enable SSL Inspection firstly and not for small business models

Features Set

Software Features

Firewall

- ICSA-certified 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 intelligence and optimization
- Content filtering 2.0
- Anti-virus, anti-malware
- Anti-spam

IPSec VPN

- ICSA-certified IPSec VPN
- Encryption: AES (256-bit), 3DES and DES
- Supports generating SHA2 Certificate
- Support route-based VPN Tunnel Interface (VTI)
- Key management: manual key, IKEv1 and IKEv2 with EAP
- Perfect forward secrecy (DH groups) support 1, 2, 5, 14
- IPSec NAT traversal
- Dead peer detection and relay detection
- PKI (X.509) certificate support

- VPN concentrator
- 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

SSL VPN

- HTTP, FTP, SMTP, POP3 and IMAP4 protocol support
- Automatic signature updates
- No file size limitation
- Supports Windows and Mac OS X
- Supports full tunnel mode
- Supports 2-step authentication
- Customizable user portal

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 Intelligence and Optimization

- 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

- Supports Kaspersky anti-virus signatures
- Identifies and blocks over 650,000 viruses
- Stream-based anti-virus engine
- HTTP, FTP, SMTP, POP3 and IMAP4 protocol support
- Automatic signature updates
- No file size limitation

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
- Firmware ZLD4.20 supports:
 - HTTPs Domain filtering
 - GeoIP Blocking
 - Monitors traffics based on country policy
 - URL blocking and keyword blocking
 - Supports to SafeSearch (SSL inspection must be enabled for this function)

SSL Inspection

- Certificate Trust Chain validation
- Support both inbound and outbound inspection
- Support Anti-virus / Content Filtering / Application intelligent / IDP inspection
- Support TLS 1.0/1.1/1.2
- Visible bypass list

Unified Security Policy

- Unified policy management interface
- Supported UTM features: anti-virus, anti-spam, IDP, content filtering 2.0, application intelligence, 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 version 1.97](#)
- Supports auto AP FW update
- Wireless L2 isolation
- Scheduled Wi-Fi 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
- Wi-Fi Multimedia (WMM) wireless QoS
- CAPWAP discovery protocol

Hotspot Management (Firmware ZLD4.20)

- 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

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

ZyXEL One Network

- ZON Utility
 - IP configuration
 - Web GUI access
 - Firmware upgrade
 - Password configuration
 - Location and System Name update
- Smart Connect
 - Discover neighboring devices
 - One-click remote management access to the neighboring ZyXEL devices

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

Device High Availability Pro (HA Pro) (Firmware ZLD4.20)

- Device failure detection and notification
- Supports ICMP and TCP ping check
- Link monitoring
- Configuration auto-sync
- Dedicated Heartbeat Link
- Instant handover
- NAT/Firewall/VPN Sessions synchronization

System Management

- Role-based administration
- Authentication: SHA-2 (512-bit), SHA-1 and MD5
- Multiple administrator logins
- Multi-lingual Web GUI (HTTPS and HTTP)
- Command line interface (console, Web console, SSH and telnet)
- Cloud CNM SecuManager*
- *Available in Sept. 2016
- SNMP v1, v2c, v3
- System configuration rollback
- Firmware upgrade via FTP, FTP-TLS and Web GUI
- Dual firmware images
- Supports Cloud Helper (Firmware ZLD4.20)

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
- Advanced reporting with Vantage Report

Licenses

Security

Product	Kaspersky Anti-Virus	Application Intelligence & IDP	Content Filtering 2.0	Anti-Spam
USG1900	1 year 2 years	1 year 2 years	1 year 2 years	1 year 2 years
USG1100				

Notes:

1. ZyXEL USGs can be purchased with bundled 12-month standard license (anti-virus, anti-spam, content filtering and IDP) with extra 1-month trial.
2. Licenses can be easily activated, renewed and managed at myZyXEL.com2.0
3. License bundles may vary according to region. Please contact your local sales representative for more information.

Connectivity & Industrial

Product	SSL VPN Tunnels	SecuExtender SSL VPN Client *1	IPSec VPN Client
USG1900	Add 5 Tunnels Add 10 Tunnels Add 50 Tunnels	For 1 client For 5 clients For 10 clients	For 1 client For 5 clients For 10 clients For 50 clients
USG1100			

*1: Support OS: MAC OS 10.7 or later



Product	Concurrent Device Upgrade	Hotspot Management*1	Managed APs	Device HA Pro	Vantage Report
USG1900	100 nodes 300 nodes	1 year/One-time	Add 4 APs Add 8 APs	One-time	For 1 device For 5 devices For 25 devices For 100 devices
USG1100					

*1: With firmware ZLD 4.20 or later

Access Point Compatibility List

Series	NWA5120 Series	NWA5000 Series	NWA3000-N Series	WAC6500 Series
	Unified Access Point	Managed Access Point	Unified Pro Access Point	Unified Pro Access Point
Models	NWA5121-NI NWA5121-N NWA5123-NI NWA5301-NJ NWA5123-AC	NWA5160N NWA5560-N NWA5550-N	NWA3160-N NWA3560-N NWA3550-N	WAC6503D-S WAC6502D-S WAC6502D-E WAC6553D-E WAC6103D-I
Functions				
Central management	Yes	Yes	Yes	Yes
Auto provisioning	Yes	Yes	Yes	Yes
Data forwarding	Local bridge	Local bridge	Local bridge	Local bridge

Accessories

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	<ul style="list-style-type: none"> • 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)
SecuExtender— SSL VPN Client 	SSL VPN client software could be installed in Windows and for MAC OS, the secured VPN connection will set-up between device and USG/ZyWALL Series.	<ul style="list-style-type: none"> • Windows XP • Windows 7 (32/64-bit) • Windows 8/8.1 (32/64-bit) • Windows 10 (32/64-bit) • MAC OS 10.7 or later

Notes:
 1. 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.
 2. SSL VPN client for Windows OS can be downloaded from official ZyXEL website. It does not require a license key to activate the application.

For more product information, visit us on the web at www.ZyXEL.com



Copyright © 2016 ZyXEL Communications Corp. All rights reserved. ZyXEL, ZyXEL logo are registered trademarks of ZyXEL Communications Corp. All other brands, product names, or trademarks mentioned are the property of their respective owners. All specifications are subject to change without notice.

