



## 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 18 APs
- ZyXEL One Network is supported

As business grows and network expands, more and more users and devices as well as new applications like cloud-based services would join the network. It means that high network availability for sustainable business, more workplace Wi-Fi and up-to-date regulations for application usages are eagerly needed. Without an effective solution to control, optimize or block social and some other Web applications, businesses would risk not only losing productivity but also exposing company network to new threats.

The new ZyXEL USG Extreme Series are Next Generation Firewalls (NGFW) designed to deliver high availability, anti-malware protection and consolidated policy enforcement for medium- to large-sized businesses and campuses. The ZyXEL USGs provides WAN and VPN load balancing and failover ensures nonstop business communications, while incorporating best-in-breed anti-virus, anti-spam, content filtering and application intelligence technology for effective application optimization and comprehensive network protection.



### Benefits

#### Powerful and Robust

ZyXEL's USG Extreme Series is built on a powerful multi-core platform to deliver high performance that helps growing businesses to overcome challenges during the expansion. In order to satisfy the needs for always-online communications, the Series features multi-WAN load balancing/failover and a comprehensive mobile broadband USB modem support list for WAN backup operations. In addition, the Series supports IPSec load balancing and failover to provide additional resiliency for the most mission-critical VPN deployments.

#### Protection and optimization

The ZyXEL USG Extreme Series provides extensive anti-malware protection and effective control of Web applications—like Facebook, Google Apps and Netflix—with industry-leading firewall, anti-virus, anti-spam, content filtering, IDP and application intelligence. These security measures are enhanced with SSL inspection, which helps block threats that are hidden in SSL encrypted connections and facilitates deeper policy enforcement.



**ZyXEL onenetwork**  
Redefining network integration

**USG1900/1100**  
Unified Security Gateway—  
Extreme Series



### Streamlined management

Unified security policy streamlines the configuration of firewall and every security feature to offer faster, easier and more consistent policy management. From a single interface, users can apply all policy criteria to every UTM feature with reduced complexity. The integrated WLAN controller also enables users to management up to 18 APs from a centralized user interface.

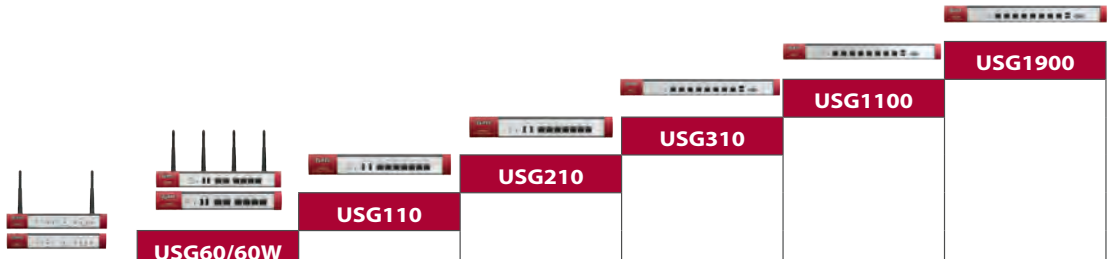
### Best TCO for Wi-Fi Expansion

Addressing the connectivity needs in the BYOD trend, the ZyXEL USG Extreme Series helps businesses deploying or expanding a managed Wi-Fi network with minimized efforts. Integrated with ZyXEL AP Controller technology, the Series enables businesses to easily scale up the WLAN and to provide seamless Wi-Fi coverage in places like meeting rooms and guest reception areas.

### 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.

### Next-Gen USG Quick Finder



Model	USG40/40W		USG60/60W		USG110	USG210	USG310	USG1100	USG1900
Description	Performance Series		Advanced Series		Advanced Series			Extreme Series	
Firewall throughput	400 Mbps	1.0 Gbps	1.6 Gbps	1.9 Gbps	5.0 Gbps	6.0 Gbps	7.0 Gbps		
VPN throughput	100 Mbps	180 Mbps	400 Mbps	500 Mbps	650 Mbps	800 Mbps	900 Mbps		
UTM throughput (AV and IDP)	50 Mbps	90 Mbps	250 Mbps	300 Mbps	400 Mbps	500 Mbps	600 Mbps		
Max. TCP concurrent sessions	20,000	40,000	60,000	80,000	100,000	500,000	500,000		
Wi-Fi	802.11 b/g/n 2.4 GHz (USG40W)	802.11 a/b/g/n Concurrent 2.4 & 5 GHz (USG60W)	-	-	-	-	-		
Managed AP number (default/max.)	2/10	2/10	2/18	2/18	2/18	2/18	2/18		
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		
Device HA	-	-	Yes	Yes	Yes	Yes	Yes		
Port grouping	Yes	Yes	Yes	Yes	-	-	-		
Single sign-on (SSO)	Yes	Yes	Yes	Yes	Yes	Yes	Yes		

### Feature Introduction



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.



VPN High  
Availability (HA)

#### VPN High Availability (HA)

ZyXEL USGs feature VPN HA to satisfy the demands of the most mission-critical VPN deployments. Supporting advanced GRE over IPSec technology, users can deploy two IPSec VPN tunnels for active-active VPN load balancing or active-passive failover.



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.



Anti-Virus

#### Anti-Virus

Powered by Kaspersky SafeStream II gateway anti-virus, ZyXEL USGs provide comprehensive and real-time protection against malware threats before they enter the network. ZyXEL USGs can identify and block over 650,000 viruses right at the gate and provide high-speed scanning with stream-based virus scanning technology.



Anti-Spam

#### Anti-Spam

With a cloud-based IP reputation system, ZyXEL anti-spam can deliver accurate, zero-hour spam outbreak protection by analyzing up-to-the-minute sender reputation data from highly diverse traffic sources. It can detect spam outbreaks in the first few minutes of emergence regardless of spam language or format.



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.



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 encryption, the ZyXEL USGs provide the most secure 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 18 APs with license upgrade.



Application  
Intelligence

#### Application Intelligence

ZyXEL's USG Extreme Series can identify, categorize and control over 3,000 social, gaming, productivity, and other Web applications and behaviors. Users can prioritize productive applications, throttle acceptable ones, and block unproductive applications to boost productivity and prevent bandwidth abuse.



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.



Content Filtering

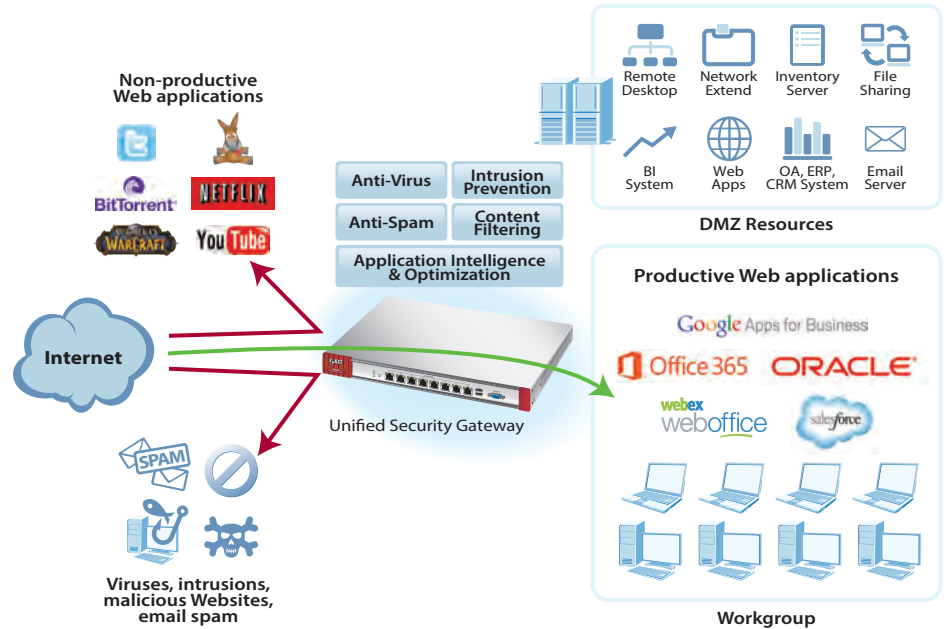
#### Content Filtering

ZyXEL content filtering helps screen access to websites that are not business related or malicious. With a massive, cloud-based database of over 140 billion URLs that are continuously analyzed and tracked, ZyXEL provides highly accurate, broad and instant protection against malicious Web content.

### Application Diagram

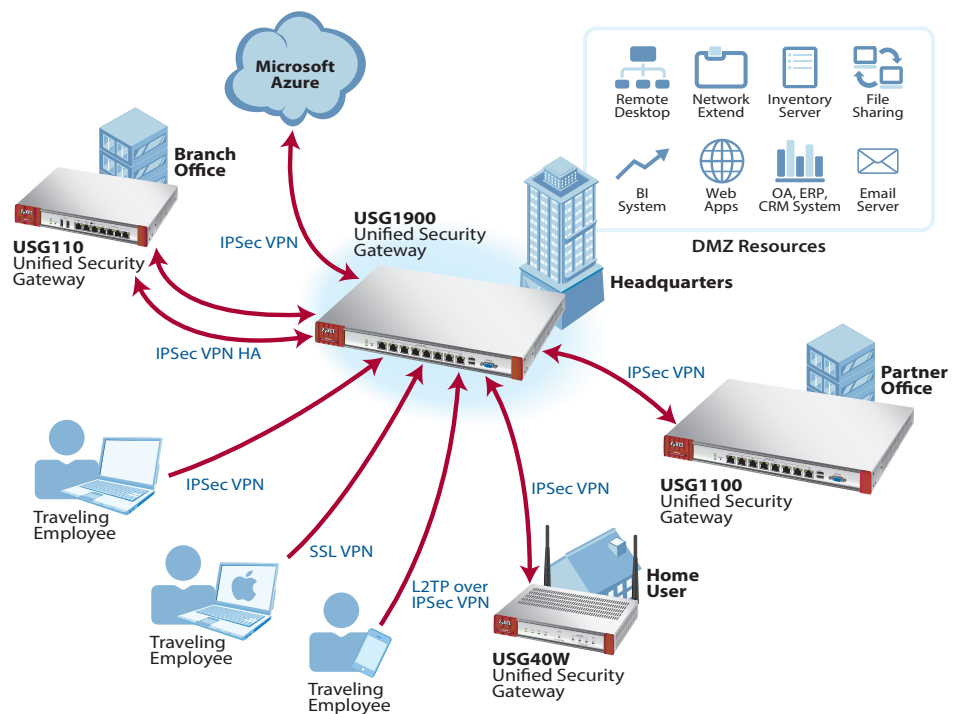
#### Anti-malware protection and application optimization

- 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



### 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 <sup>*1</sup>			
SPI firewall throughput (Mbps) <sup>*2</sup>	7,000	6,000	
VPN throughput (Mbps) <sup>*3</sup>	900	800	
IDP throughput (Mbps) <sup>*4</sup>	650	550	
AV throughput (Mbps) <sup>*4</sup>	600	500	
UTM throughput (AV and IDP) <sup>*4</sup>	600	500	
Unlimited user licenses	Yes	Yes	
Max. TCP concurrent sessions <sup>*5</sup>	500,000	500,000	
Max. concurrent IPsec VPN tunnels <sup>*8</sup>	2,000	1,000	
Max. concurrent SSL VPN users <sup>*6</sup>	750	500	
Included SSL VPN user no. <sup>*6</sup>	250	250	
Customizable zones	Yes	Yes	
IPv6 support	Yes	Yes	
VLAN interface	128	128	
WLAN Management <sup>*7</sup>			
AP Controller (APC) support	Yes	Yes	
Managed AP number (default/max.)	2/18	2/18	
Key Software Features			
Firewall	Yes	Yes	
Virtual private network (VPN)	Yes (IPSec, SSL, L2TP over IPSec)	Yes (IPSec, SSL, L2TP over IPSec)	
Anti-virus (AV)	Yes	Yes	
Intrusion detection and prevention (IDP)	Yes	Yes	
Anti-spam	Yes	Yes	
Content filtering (CF)	Yes	Yes	
HA	Yes	Yes	
Bandwidth 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	560,811.5
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:

\*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: With firmware ZLD 4.13 or later.

\*7: With firmware ZLD 4.11 or later.

\*8: Including Gateway-to-Gateway and Client-to-Gateway



## 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
- Anti-virus, anti-malware
- Anti-spam

#### IPsec VPN

- ICSA-certified IPsec VPN
- Encryption: AES (256-bit), 3DES and DES
- Authentication: SHA-2 (512-bit), SHA-1 and MD5
- Key management: manual key, IKEv1 and IKEv2 with EAP
- Perfect forward secrecy (DH groups) support 1, 2, 5
- 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

- 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
- SSL (HTTPS) inspection support

#### Application Intelligence and Optimization

- Granular control over the most important applications
- Identifies and controls over 3,000 applications and behaviors
- Supports over 15 application categories
- Application bandwidth management
- Supports user authentication
- Real-time statistics and reports
- SSL (HTTPS) inspection support
- 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
- SSL (HTTPS) inspection support

#### 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

- 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
- SSL (HTTPS) inspection support

#### Unified Security Policy

- Unified policy management interface
- Supported UTM features: anti-virus, anti-

- spam, IDP, content filtering, 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 1.95](#)
- 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

#### Mobile Broadband

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

\* 4G USB modem support available in future firmware upgrades

#### 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

#### ZyXEL One Network

- ZON Utility
  - IP configuration
  - Web GUI access
  - Firmware upgrade
  - Password configuration
- 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 (HA)

- Active-passive failover mode
- Device failure detection and notification
- Supports ICMP and TCP ping check
- Link monitoring
- Configuration auto-sync

### System Management

- Role-based administration
- Multiple administrator logins
- Multi-lingual Web GUI (HTTPS and HTTP)
- Command line interface (console, Web console, SSH and telnet)
- CloudCNM support starting from ZLD4.13

- SNMP v2c (MIB-II)
- System configuration rollback
- Firmware upgrade via FTP, FTP-TLS and Web GUI
- Dual firmware images

### 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	Anti-Spam
USG1900	1 year 2 years	1 year 2 years	1 year 2 years	1 year 2 years
USG1100	1 year 2 years	1 year 2 years	1 year 2 years	1 year 2 years

#### 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.

### VPN, Management and Reporting

Product	SSL VPN Tunnels	SecureExtender SSL VPN Client <sup>*1</sup>	IPSec VPN Client	Managed APs <sup>*2</sup>	Vantage Report
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	Add 8 APs	For 1 device For 5 devices For 25 devices For 100 devices
USG1100					



\*1: Support OS: MAC OS 10.7 or later

\*2: With firmware ZLD 4.10 or later

## Access Point Compatibility List

Series	NWA5120 Series	NWA5000 Series	NWA3000-N Series
	Unified Access Point	Managed Access Point	Unified Pro Access Point
Models	NWA5121-NI NWA5121-N NWA5123-NI	NWA5160N NWA5560-N NWA5550-N	NWA3160-N NWA3560-N NWA3550-N
Functions			
Central management	Yes	Yes	Yes
Auto provisioning	Yes	Yes	Yes
Data forwarding	Local bridge	Local bridge	Local bridge

### Accessories

Item	Description	Supported OS
<b>IPSec VPN Client</b> 	IPSec VPN client software for the ZyWALL and USG Series with Easy VPN for zero-configuration remote access	<ul style="list-style-type: none"> <li>• Windows XP (32-bit)</li> <li>• Windows Server 2003 (32-bit)</li> <li>• Windows Server 2008 (32/64-bit)</li> <li>• Windows Vista (32/64-bit)</li> <li>• Windows 7 (32/64-bit)</li> <li>• Windows 8 (32/64-bit)</li> </ul>
<b>SecuExtender—SSL VPN Client</b> 	SSL VPN client software for the ZyWALL and USG Series with auto-installation in Windows, and lite set up for MAC user	<ul style="list-style-type: none"> <li>• Windows OS</li> <li>• MAC OS 10.7 or later</li> </ul>

**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 is pushed from USG/ZyWALL device and launches automatically. It does not require a license key to activate the application.

For more product information, visit us on the web at [www.ZyXEL.com](http://www.ZyXEL.com)



Copyright © 2015 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.

