More and more people are relying on smart devices and cloud-based applications for business communications. This means that high network availability is critical for business continuity, more Wi-Fi is demanded in the workplace, and traditional regulatory measures for application usage are obsolete. Without an effective solution to control, optimize and block social, productivity and other Web applications, SMBs risk losing work productivity and exposing company networks to new Web threats.

The new ZyXEL USG Advanced Series are Next Generation Firewalls (NGFW) designed to meet the mobility, anti-malware and policy enforcement challenges in SMBs. The integrated WLAN controller offers easy WLAN scalability for the growing demand for Wi-Fi; while WAN and VPN load balancing and failover ensures non-stop business communications. ZyXEL USGs offer industry-leading anti-virus, anti-spam, content filtering and application intelligence technology for effective application optimization and comprehensive network protection.

Benefits

**Always online**

The ZyXEL USG Advanced Series offers SMBs high network availability for always online communications. It features multi-WAN load balancing and failover, and a comprehensive mobile broadband USB modem support list for WAN backup. On top of that, the Series supports IPSec load balancing and failover to provide added resiliency for the most mission-critical VPN deployments.

**Protection and optimization**

The ZyXEL USG Advanced 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.

- High-performance, high-value Next Generation Firewall (NGFW) for small and medium-sized businesses
- 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)
- Built-in WLAN controller for centralized AP management and effortless WLAN scalability of up to 18 APs
- Comprehensive mobile broadband USB modem compatibility and multi-WAN load-balancing, failover and fail back support

Secure and Always Online Networking for Small- to Medium-sized Businesses

USG310/210/110
Unified Security Gateway—Advanced 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.

More Wi-Fi
Addressing the trend of BYOD, the ZyXEL USG Advanced Series helps SMBs satisfy the Wi-Fi demand for an exploding amount of smart devices. The Series is integrated with a WLAN controller that enables businesses to easily scale up the WLAN and provide Wi-Fi in multiple areas like meeting rooms and guest reception areas.

Next-Gen USG Advanced Series

USG310
Unified Security Gateway
8 x GbE RJ-45, 2 x USB (multi-WAN & mobile broadband)

USG110
Unified Security Gateway
7 x GbE RJ-45, 2 x USB (multi-WAN & mobile broadband)

USG210
Unified Security Gateway
7 x GbE RJ-45, 2 x USB (multi-WAN & mobile broadband)

USG210
Unified Security Gateway
7 x GbE RJ-45, 2 x USB (multi-WAN & mobile broadband)

Next-Gen USG Quick Finder

<table>
<thead>
<tr>
<th>Model</th>
<th>USG40/40W</th>
<th>USG60/60W</th>
<th>USG110</th>
<th>USG210</th>
<th>USG310</th>
<th>USG1100</th>
<th>USG1900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Performance Series</td>
<td>Advanced Series</td>
<td>Extreme Series</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall throughput</td>
<td>400 Mbps</td>
<td>1.0 Gbps</td>
<td>1.6 Gbps</td>
<td>1.9 Gbps</td>
<td>5.0 Gbps</td>
<td>6.0 Gbps</td>
<td>7.0 Gbps</td>
</tr>
<tr>
<td>VPN throughput</td>
<td>100 Mbps</td>
<td>180 Mbps</td>
<td>460 Mbps</td>
<td>500 Mbps</td>
<td>650 Mbps</td>
<td>800 Mbps</td>
<td>900 Mbps</td>
</tr>
<tr>
<td>UTM throughput [AV and IDP]</td>
<td>50 Mbps</td>
<td>90 Mbps</td>
<td>250 Mbps</td>
<td>300 Mbps</td>
<td>400 Mbps</td>
<td>500 Mbps</td>
<td>600 Mbps</td>
</tr>
<tr>
<td>Max. TCP concurrent sessions</td>
<td>20,000</td>
<td>40,000</td>
<td>60,000</td>
<td>80,000</td>
<td>100,000</td>
<td>300,000</td>
<td>500,000</td>
</tr>
<tr>
<td>Recommended # of users</td>
<td>1 - 10</td>
<td>10 - 25</td>
<td>25 - 50</td>
<td>50 - 75</td>
<td>75 - 200</td>
<td>200 - 350</td>
<td>350 - 500</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>802.11 b/g/n 2.4 GHz</td>
<td>802.11 a/b/g/n Concurrent 2.4 &amp; 5 GHz</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Managed AP number (default/max.)</td>
<td>2/10</td>
<td>2/10</td>
<td>2/18</td>
<td>2/18</td>
<td>2/18</td>
<td>2/18</td>
<td>2/18</td>
</tr>
<tr>
<td>UTM licenses</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Multi-WAN</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Unified security policy</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SSL inspection</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Device HA</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Port grouping</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Multi-WAN & Mobile Broadband
The ZyXEL USG Advanced 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)
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 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
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
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.

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
The integrated WLAN controller supports CAPWAP, and enables centralized authentication and access management of multiple APs in the network. The ZyXEL USG Advanced Series can manage 2 APs by default, and up to 18 APs with license upgrade.

Application Intelligence
ZyXEL’s USG Advanced 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 enables the ZyXEL Advanced 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
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 additionally 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 headquarters USG/ZyWALL can also establish an IPSec VPN connection with Microsoft Azure for secured access to a variety of cloud-based applications.
## Specifications

<table>
<thead>
<tr>
<th>Model</th>
<th>USG310</th>
<th>USG210</th>
<th>USG110</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware Specifications</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/100/1000 Mbps RJ-45 ports</td>
<td>8 (configurable)</td>
<td>4 x LAN/DMZ, 2 x WAN, 1 x OPT</td>
<td>4 x LAN/DMZ, 2 x WAN, 1 x OPT</td>
</tr>
<tr>
<td>USB ports</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Console port</td>
<td>Yes (DB9)</td>
<td>Yes (DB9)</td>
<td>Yes (DB9)</td>
</tr>
<tr>
<td>Rack-mountable</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>System Capacity &amp; Performance</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPI firewall throughput (Mbps)*1</td>
<td>5,000</td>
<td>1,900</td>
<td>1,600</td>
</tr>
<tr>
<td>VPN throughput (Mbps)*2</td>
<td>650</td>
<td>500</td>
<td>400</td>
</tr>
<tr>
<td>IDP throughput (Mbps)*3</td>
<td>450</td>
<td>350</td>
<td>300</td>
</tr>
<tr>
<td>AV throughput (Mbps)*4</td>
<td>400</td>
<td>300</td>
<td>250</td>
</tr>
<tr>
<td>UTM throughput (AV and IDP)*4</td>
<td>400</td>
<td>300</td>
<td>250</td>
</tr>
<tr>
<td>Unlimited user licenses</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Max. TCP concurrent sessions*3</td>
<td>100,000</td>
<td>80,000</td>
<td>60,000</td>
</tr>
<tr>
<td>New TCP session rate</td>
<td>12,000</td>
<td>3,500</td>
<td>3,500</td>
</tr>
<tr>
<td>Max. concurrent IPSec VPN tunnels</td>
<td>300</td>
<td>200</td>
<td>100</td>
</tr>
<tr>
<td>Max. concurrent SSL VPN users</td>
<td>105</td>
<td>50</td>
<td>25</td>
</tr>
<tr>
<td>Included SSL VPN user no.</td>
<td>25</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>Customizable zones</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IPv6 support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>VLAN interface</td>
<td>64</td>
<td>32</td>
<td>16</td>
</tr>
<tr>
<td><strong>Management</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AP Controller (APC) ver.</td>
<td>2/18</td>
<td>2/18</td>
<td>2/18</td>
</tr>
<tr>
<td>Managed AP number (default/max.)</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
</tr>
<tr>
<td><strong>Key Software Features</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtual Private Network (VPN)</td>
<td>Yes (IPSec, SSL, L2TP over IPSec)</td>
<td>Yes (IPSec, SSL, L2TP over IPSec)</td>
<td>Yes (IPSec, SSL, L2TP over IPSec)</td>
</tr>
<tr>
<td>Firewall</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Anti-Virus (AV)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Anti-spam</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Content Filtering (CF)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Application intelligence and optimization</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Intrusion Detection and Prevention (IDP)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SSL inspection</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Single Sign-On (SSO)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>WLAN controller</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Power Requirements</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power input</td>
<td>100 - 240 V AC, 50/60 Hz, 1.3 A max.</td>
<td>12 V DC, 3.33 A max.</td>
<td>12 V DC, 3.33 A max.</td>
</tr>
<tr>
<td>Max. power consumption (watt)</td>
<td>58.5</td>
<td>37.0</td>
<td>37.0</td>
</tr>
<tr>
<td><strong>Physical Specifications</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dimensions (WxDxH)(mm/in.)</td>
<td>430 x 250 x 44/16.93 x 9.84 x 1.73</td>
<td>300 x 178 x 44/11.81 x 7 x 1.73</td>
<td>300 x 178 x 44/11.81 x 7 x 1.73</td>
</tr>
<tr>
<td>Weight (kg/lb.)</td>
<td>3.3/7.28</td>
<td>2/4.4</td>
<td>2/4.4</td>
</tr>
<tr>
<td><strong>Packing</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dimensions (WxDxH)(mm/in.)</td>
<td>519 x 392 x 163/20.43 x 15.43 x 6.42</td>
<td>351 x 149 x 243/13.82 x 5.87 x 9.57</td>
<td>351 x 149 x 243/13.82 x 5.87 x 9.57</td>
</tr>
<tr>
<td>Weight (kg/lb.)</td>
<td>4.8/10.58</td>
<td>3.264/7.20</td>
<td>3.264/7.20</td>
</tr>
<tr>
<td><strong>Included accessories</strong></td>
<td>Power cord</td>
<td>Power adapter</td>
<td>Power adapter</td>
</tr>
<tr>
<td></td>
<td>Rack mounting kit</td>
<td>Rack mounting kit</td>
<td>Rack mounting kit</td>
</tr>
<tr>
<td><strong>Environmental Specifications</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>0°C to 40°C (32°F to 104°F)</td>
<td>0°C to 40°C (32°F to 104°F)</td>
<td>0°C to 40°C (32°F to 104°F)</td>
</tr>
<tr>
<td>Humidity</td>
<td>10% to 90% (non-condensing)</td>
<td>10% to 90% (non-condensing)</td>
<td>10% to 90% (non-condensing)</td>
</tr>
<tr>
<td>Storage Temperature</td>
<td>-30°C to 70°C (-22°F to 158°F)</td>
<td>-30°C to 70°C (-22°F to 158°F)</td>
<td>-30°C to 70°C (-22°F to 158°F)</td>
</tr>
<tr>
<td>Humidity</td>
<td>10% to 90% (non-condensing)</td>
<td>10% to 90% (non-condensing)</td>
<td>10% to 90% (non-condensing)</td>
</tr>
<tr>
<td><strong>MTBF (hr)</strong></td>
<td>560,811.5</td>
<td>787,109.3</td>
<td>787,109.3</td>
</tr>
<tr>
<td><strong>Certifications</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMC</td>
<td>FCC Part 15 (Class A), CE EMC (Class A), C-Tick (Class A), BSMI</td>
<td>FCC Part 15 (Class A), CE EMC (Class A), C-Tick (Class A), BSMI</td>
<td>FCC Part 15 (Class A), CE EMC (Class A), C-Tick (Class A), BSMI</td>
</tr>
<tr>
<td>Safety</td>
<td>LVD (EN60950-1), BSMI</td>
<td>LVD (EN60950-1), BSMI</td>
<td>LVD (EN60950-1), BSMI</td>
</tr>
</tbody>
</table>

*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: SPI firewall 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.
Features Set

Software Features

Firewall
- ICSA-certified firewall (certification in progress)
- 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

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

IPv6 Support
- IPv6 Ready gold logo (certification in progress)
- Dual stack
- IPv4 tunneling (6rd and 6to4 transition tunnel)
- IPv6 addressing
- DNS
- DCHPv6
- 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 (certification in progress)
- 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

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

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

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

WLAN Management
- ZyXEL AP Controller (APC) 1.0 compliant
- Client RSSI threshold to prevent sticky clients
- 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
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)
- 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

<table>
<thead>
<tr>
<th>Product</th>
<th>Kaspersky Anti-Virus</th>
<th>Application Intelligence &amp; IDP</th>
<th>Content Filtering</th>
<th>Anti-Spam</th>
</tr>
</thead>
<tbody>
<tr>
<td>USG310</td>
<td>1 year</td>
<td>1 year</td>
<td>1 year</td>
<td>1 year</td>
</tr>
<tr>
<td></td>
<td>2 years</td>
<td>2 years</td>
<td>2 years</td>
<td>2 years</td>
</tr>
<tr>
<td>USG210</td>
<td>1 year</td>
<td>1 year</td>
<td>1 year</td>
<td>1 year</td>
</tr>
<tr>
<td></td>
<td>2 years</td>
<td>2 years</td>
<td>2 years</td>
<td>2 years</td>
</tr>
<tr>
<td>USG110</td>
<td>1 year</td>
<td>1 year</td>
<td>1 year</td>
<td>1 year</td>
</tr>
<tr>
<td></td>
<td>2 years</td>
<td>2 years</td>
<td>2 years</td>
<td>2 years</td>
</tr>
</tbody>
</table>

Notes:
1. ZyXEL USGs can be purchased with bundled 12-month standard license (anti-virus, anti-scam, content filtering and IDP) with extra 1-month trial.
2. Licenses can be easily activated, renewed and managed at myZyXEL.com 2.0
3. License bundles may vary according to region. Please contact your local sales representative for more information.

VPN, Management and Reporting

<table>
<thead>
<tr>
<th>Product</th>
<th>Managed APs</th>
<th>SecuExtender—SSL VPN Client</th>
<th>IPSec VPN Client</th>
<th>Vantage Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>USG310</td>
<td>Add 8 APs</td>
<td>Add 10 clients</td>
<td>For 1 client</td>
<td>For 1 device</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For 5 clients</td>
<td>For 5 devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For 10 clients</td>
<td>For 25 devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For 50 clients</td>
<td>For 100 devices</td>
</tr>
<tr>
<td>USG210</td>
<td>Add 8 APs</td>
<td>Add 10 clients</td>
<td></td>
<td></td>
</tr>
<tr>
<td>USG110</td>
<td>Add 8 APs</td>
<td>Add 10 clients</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Access Point Compatibility List

<table>
<thead>
<tr>
<th>Series</th>
<th>NWA5120 Series</th>
<th>NWA5000 Series</th>
<th>NWA3000-N Series</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Unified Access Point</td>
<td>Managed Access Point</td>
<td>Unified Pro Access Point</td>
</tr>
<tr>
<td>Model</td>
<td>NWA5121-NI</td>
<td>NWA5160N</td>
<td>NWA3160N</td>
</tr>
<tr>
<td></td>
<td>NWA5123-N</td>
<td>NWA5560-N</td>
<td>NWA3560-N</td>
</tr>
<tr>
<td></td>
<td>NWA5123-NI</td>
<td>NWA5550-N</td>
<td>NWA3550-N</td>
</tr>
</tbody>
</table>

Functions

| Central management  | Yes  | Yes  | Yes  |
| Auto provisioning   | Yes  | Yes  | Yes  |
| Data forwarding     | Local bridge | Local bridge | Local bridge |
## Accessories

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Supported OS</th>
</tr>
</thead>
</table>
| **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) |
| **SecuExtender—SSL VPN Client** | SSL VPN client software for the ZyWALL and USG Series with auto-installation in Windows, and lite set up for MAC user | • Windows OS  
• 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 is pushed from USG/ZyWALL device and launches automatically. It does not require a license key to activate the application.