Enterprise Security
ZyWALL Unified Security Gateway Series
(20/50/100/200/300/1000/2000 Series)

Key Features
- All-new platform: “3rd” generation ZyWALL
- USG clean-traffic architecture
- New generation UTM solution (except USG 20/20W)
- Robust hybrid VPN (IPSec and SSL)
- Application firewall (except USG 20/20W)
- Granular control over social networking applications
- Non-stop Internet access with multiple WAN and 3G backups
- ICsA firewall, IPSec certification
- Comprehensive report system
- Anti-Spam service
- ZyXEL Security Distribution Network (2SDN)

Key Benefits
- Secure connectivity
- Given the prevalence and importance of information technology (IT) systems today and the nature and scale of both the opportunities and risks associated with significant deployments of new networking technologies, organizations are forced to evaluate solutions to build up a safer infrastructure to secure online transactions, in which involve exchange of valuable information. The infrastructure should be tailored to meet operation requirements for expanding remote sites as well as mobile teleworkers.

Proactive protection
- Malicious virus, worm, exploits could cripple corporate networks and halt business transactions. In addition to severe financial loss, you also risk leakage of confidential information. As mass-mailing software companies mushroom on the Internet, your network is bombarded with massive amounts of junk mail spam). Without intelligent detection and proactive blocking, users have to go through the tedious and time-consuming task of sifting through the overflowing mailbox, and such scenario leads to serious productivity loss.

Policy compliance
- With numerous file-sharing (P2P) and Instant Messaging (IM) applications, it is easier for company employees to share files and chat online during work hours. Rapid file sharing not only compromises network safety with the sharing of questionable files containing malicious viruses, but may also violate copyright issues and create legal hazards.

Network resilience
- ISP links broken, hardware and software failure on the gateway, dead VPN tunnels — these are severe challenges IT staff face when designing the network infrastructure. In short, we need to take fault tolerance on the network path into consideration when building up a highly available network infrastructure for non-stop operations.

Manageability
- With ZyXEL’s CNA (Centralized Network Management), users can achieve the following objects:
  - Easy VPN management and diagnostic capability
  - Complete security policies and UTM management
  - Low TCO of massive deployment and device maintenance
  - Active monitoring, alerting and comprehensive graphic reports

The solution provides an efficient centralized management system for enterprises of any size to reduce operational costs regardless of the number of branch offices or remote locations.

Cost-effectiveness
- With the adoption of ZyXEL’s USG device, the follow costs can be saved:
  - Device hardware maintenance fee: ZyXEL provides a one more year hardware warranty out of factory.
  - Free software upgrade now ZyXEL provides free software upgrade for you to enjoy complete protection without additional expense.

Security Licenses

<table>
<thead>
<tr>
<th>Product</th>
<th>Duration</th>
<th>ZyWALL Anti-Virus</th>
<th>Kaspersky Anti-Virus</th>
<th>IDP</th>
<th>Content Filter</th>
<th>Vantage CNM</th>
<th>Vantage Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>USG 2000</td>
<td>1 year</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>All ZyWALL Models support, 10 modes 25 nodes 30 modes 100 nodes 1000 nodes</td>
<td>2 to 25 SSL Tunnels</td>
</tr>
<tr>
<td>USG 1000</td>
<td>1 year</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>All ZyWALL Models support, 1 device 5 devices 25 devices 100 devices</td>
<td></td>
</tr>
<tr>
<td>USG 300</td>
<td>1 year</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>All ZyWALL Models support, 10 modes 25 nodes 30 modes 100 nodes 1000 nodes</td>
<td></td>
</tr>
<tr>
<td>USG 200</td>
<td>2 years</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>All ZyWALL Models support, 10 modes 25 nodes 30 modes 100 nodes 1000 nodes</td>
<td></td>
</tr>
<tr>
<td>USG 100</td>
<td>2 years</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>All ZyWALL Models support, 10 modes 25 nodes 30 modes 100 nodes 1000 nodes</td>
<td></td>
</tr>
</tbody>
</table>

3G Card Support

3G cards are not included. Please visit http://www.zyxel.com/web/ and find the following path:
Internet Security Appliance → Unified Security Gateway → the individual USG product pages to see the 3G Card Compatibility List for supported USB devices.

*Available in Q3 2017*
Outbound Threats
BWM products support the Gigabit Ethernet.
Virus (include Kaspersky Anti-Virus & ZyXEL Management security features such as Anti-
provides integrated Unified Threat layer threat protection for small businesses industry-leading performance and multi-
accelerator, the ZyWALL USG Series delivers high-performance SecuASIC technology acceleration technology in one box. Powered
ZyXEL USG Series is built with a powerful Integrated High Performance Security architecture, a performance proven architecture for gigabit fiber. It provides real-time inspection to prevent network
from threats without sacrificing performance. Company network is not only flawlessly secured but also greatly enhanced on performance to improve operational productivity and efficiency when applications such as file-loading, emailing, and information searches are processed at higher speed. Take USG 50 as an example, USG 50 delivers excellent performance to meet small business.

New generation UTM solution
The ZyWALL USG Series deploys hardware-acceleration technology in one box. Powered by high-performance SecuASIC technology and a hardware-based encryption accelerator, the ZyWALL USG Series delivers industry-leading performance and multi-layer threat protection for small businesses and enterprises. The ZyWALL USG Series provides integrated Unified Threat Management security features such as Anti-Virus (include Kaspersky Anti-Virus & ZyXEL Anti-Virus), IDP, Anti-Spam, Content Filtering and Firewall/WAN. All ZyWALL USG Series products support the Gigabit Ethernet.

Key Applications
ZyWALL USG clean-traffic architecture
The ZyWALL USG’s clean-traffic architecture protects against network risks such as viruses, worms, Trojan Horses, spyware, phishing attacks and other emerging Internet threats. With the clean-traffic architecture, enterprises users are assured to have clean and secure network environments.

Endpoint security
With the new Endpoint Security feature (EPS), administrators can easily identify “bad” users, i.e. where no AV software has been installed. By enforcing installation of the Anti-Virus software, the ZyWALL mitigates the threat of virus outbreaks and thus the loss of money and employee productivity. The EPS supports Norton*, Kaspersky* and TrendMicro*. All client software, among others. Additionally, personal firewall software such as Kaspersky Internet Security 2009/2010, Windows Firewall and TrendMicro PC-Cillin/Internet Security 2010 are also supported with the new EPS feature.

High performance
ZyXEL USG Series is built with a powerful Integrated High Performance Security architecture, a performance proven architecture for gigabit fiber. It provides real-time inspection to prevent network from threats without sacrificing performance. Company network is not only flawlessly secured but also greatly enhanced on performance to improve operational productivity and efficiency when applications such as file-loading, emailing, and information searches are processed at higher speed. Take USG 50 as an example, USG 50 delivers excellent performance to meet small business.

High performance
ZyXEL USG Series is built with a powerful Integrated High Performance Security architecture, a performance proven architecture for gigabit fiber. It provides real-time inspection to prevent network from threats without sacrificing performance. Company network is not only flawlessly secured but also greatly enhanced on performance to improve operational productivity and efficiency when applications such as file-loading, emailing, and information searches are processed at higher speed. Take USG 50 as an example, USG 50 delivers excellent performance to meet small business.

High performance
ZyXEL USG Series is built with a powerful Integrated High Performance Security architecture, a performance proven architecture for gigabit fiber. It provides real-time inspection to prevent network from threats without sacrificing performance. Company network is not only flawlessly secured but also greatly enhanced on performance to improve operational productivity and efficiency when applications such as file-loading, emailing, and information searches are processed at higher speed. Take USG 50 as an example, USG 50 delivers excellent performance to meet small business.
Non-stop Internet access with multiple WAN and 3G backups

The ZyWALL USG not only supports multiple WAN ports but also 3G through USB or PCMCIA cards. This feature enables "active-active" load sharing or "active-passive" failover configuration to deliver highly reliable network connectivity.

Granular control over social networking applications

Social networking applications such as Facebook, Twitter, and Youtube have become an Internet phenomenon to connect people quickly and to share information. Without flexible management, social networking applications will eat up business productivity. ZyWALL USG ensures that the Internet is not abused to prevent bandwidth to be wasted or human resource policy violations. ZyWALL USG provides granular control over social networking applications.

Application firewall

More and more network applications bring malicious software into your office. This kind of unwanted software, especially IM/P2P applications, may cause bandwidth waste or even system damage. Using the application patrol and bandwidth management features, you can have full control over traffic blocking or rate limit settings.

Enterprise Security
ZyWALL Unified Security Gateway Series
(20/50/100/200/300/1000/2000 Series)
**Enterprise Security**

**ZyWALL Unified Security Gateway Series**

*(20/50/100/200/300/1000/2000 Series)*

---

**High availability**

High availability is essential in enterprise networks. It ensures a system or component can be continuously operational for a desirable long length of time.

The ZyWALL USG Series provide high availability feature as:

- Multiple WAN ports and configure load balancing between these ports.
- An auxiliary (backup) Internet connection as known as out of band Management.
- A backup ZyWALL in the event the master ZyWALL fails (device HA).

To minimize the impact of single-point failures, the ZyWALL USG Series supports device HA (High Availability) to assure network availability.

---

**Comprehensive reporting system**

The ZyWALL USG Series has a built-in reporting system that offers a comprehensive set of real-time and historical reports including firewall, virus and intrusion attacks, bandwidth usage, Web site usage and user activities. Furthermore, with Vantage Report (VRPT), a Web-based reporting system, administrators can easily collect traffic data and analyze a distributed network for their organizations to become more aware of suspicious activities and to ensure better business productivity.

---

**Anti-Spam service**

ZyXEL’s Anti-Spam service eliminates spam, phishing, virus and malware threats through a unified security architecture without dropping legitimate messages. With ZyXEL’s Anti-Spam service, enterprises can save time and resources dealing with unwanted email to reduce operational costs.

---

**ZyXEL Security Distribution Network (ZSDN) ensures rapid response to new threats**

ZSDN Provides Up-to-Date Protection

- The myZyXEL.com Web site delivers a convenient, centralized way to register all ZyWALL units and Security Services.
- The ZyXEL Security Update Servers operates 24x7 to automatically deliver updated signature databases to ZyWALL units around the world.
- The mySecurityZone portal provides comprehensive, searchable information regarding viruses and system vulnerabilities, and it provides a wealth of information resources that keep customers up-to-date on the latest vulnerabilities and countermeasures.
# Specifications

## ZyWALL Unified Security Gateway Series

### (20/50/100/200/300/1000/2000 Series)

### Model

<table>
<thead>
<tr>
<th>Model</th>
<th>ZyWALL USG 20W</th>
<th>ZyWALL USG 20</th>
<th>ZyWALL USG 50</th>
<th>ZyWALL USG 100</th>
<th>ZyWALL USG 200</th>
<th>ZyWALL USG 600</th>
<th>ZyWALL USG 1000</th>
<th>ZyWALL USG 2000</th>
</tr>
</thead>
</table>

### Features

- Unified Security Gateway for SB (1~5 PC Users)
- All Gigabit Ethernet interface hardware design
- High-performance multi-layer threat protection
- Hybrid VPN (IPSec, SSL) secures connection
- 3G USB dongle as the backup WAN
- 802.11/b/g/n wireless AP

- Unified Security Gateway for SB (1~10 PC Users)
- All Gigabit Ethernet interface hardware design
- High-performance multi-layer threat protection
- Hybrid VPN (IPSec, SSL) secures connection
- 3G USB dongle as the backup WAN

- Unified Security Gateway for SMB (25~50 PC Users)
- High-performance multi-layer threat protection
- Hybrid VPN (IPSec, SSL and L2TP) secures connection to headquarters
- Support Kaspersky and ZyXEL anti-virus

- Unified Security Gateway for SMB (50~75 PC Users)
- High-performance multi-layer threat protection
- Hybrid VPN (IPSec, SSL and L2TP) secures connection to headquarters
- Support Kaspersky and ZyXEL anti-virus

- Unified Security Gateway for SMB (75~200 PC Users)
- High-performance multi-layer threat protection
- Hybrid VPN (IPSec, SSL and L2TP) secures connection to headquarters
- Support Kaspersky and ZyXEL anti-virus

- Unified Security Gateway for SMB (200~500 PC Users)
- High-performance multi-layer threat protection
- Hybrid VPN (IPSec, SSL and L2TP) secures connection to headquarters
- Support Kaspersky and ZyXEL anti-virus

### Hardware Specifications

#### 1/10/100/1000 Interfaces (Copper)

<table>
<thead>
<tr>
<th>Model</th>
<th>4 x LAN/DMZ, 1 x WAN</th>
<th>4 x LAN/DMZ, 1 x WAN</th>
<th>5 x LAN/DMZ, 2 x WAN</th>
<th>5 x LAN/DMZ, 2 x WAN, 1 x OPT</th>
</tr>
</thead>
</table>

#### Dual Personality GE (SP/UPK)

<table>
<thead>
<tr>
<th>Model</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
</tr>
</thead>
</table>

#### USB Ports

<table>
<thead>
<tr>
<th>Model</th>
<th>1</th>
<th>2</th>
<th>2</th>
<th>2</th>
</tr>
</thead>
</table>

#### SEM Slot (Security Extension Module)

<table>
<thead>
<tr>
<th>Model</th>
<th>-</th>
<th>-</th>
<th>-</th>
<th>-</th>
</tr>
</thead>
</table>

#### Card Slot

<table>
<thead>
<tr>
<th>Model</th>
<th>-</th>
<th>-</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
</table>

#### 802.11/b/g/n Mbps

<table>
<thead>
<tr>
<th>Model</th>
<th>1/2</th>
<th>-</th>
<th>-</th>
<th>-</th>
</tr>
</thead>
</table>

#### 2x2 Antenna

<table>
<thead>
<tr>
<th>Model</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
</tr>
</thead>
</table>

#### SPI Firewall Throughput*, Mbps

<table>
<thead>
<tr>
<th>Model</th>
<th>60</th>
<th>50</th>
<th>120</th>
<th>120</th>
</tr>
</thead>
</table>

#### VPN Throughput (3DES)*, Mbps

<table>
<thead>
<tr>
<th>Model</th>
<th>60</th>
<th>50</th>
<th>120</th>
<th>120</th>
</tr>
</thead>
</table>

#### UTM Throughput (K=128)*, Mbps

<table>
<thead>
<tr>
<th>Model</th>
<th>60</th>
<th>50</th>
<th>120</th>
<th>120</th>
</tr>
</thead>
</table>

#### WiFi Throughput, Mbps

<table>
<thead>
<tr>
<th>Model</th>
<th>60</th>
<th>50</th>
<th>120</th>
<th>120</th>
</tr>
</thead>
</table>

#### Unlimited User Licenses

<table>
<thead>
<tr>
<th>Model</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
</tr>
</thead>
</table>

#### Max. Sessions*2

<table>
<thead>
<tr>
<th>Model</th>
<th>6,000</th>
<th>6,000</th>
<th>10,000</th>
<th>20,000</th>
</tr>
</thead>
</table>

#### New Session Rate*3

<table>
<thead>
<tr>
<th>Model</th>
<th>900</th>
<th>900</th>
<th>1,000</th>
<th>1,000</th>
</tr>
</thead>
</table>

#### Max. Concurrent IPSec VPN Tunnels

<table>
<thead>
<tr>
<th>Model</th>
<th>2</th>
<th>2</th>
<th>2</th>
<th>2</th>
</tr>
</thead>
</table>

#### Max. Concurrent SSL VPN Users

<table>
<thead>
<tr>
<th>Model</th>
<th>1</th>
<th>5</th>
<th>5</th>
<th>5</th>
</tr>
</thead>
</table>

#### Customized Zones

<table>
<thead>
<tr>
<th>Model</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
</tr>
</thead>
</table>

### Power Requirement

<table>
<thead>
<tr>
<th>Power Requirement</th>
<th>100<del>240 VAC, 50</del>60 Hz, 1.2 A</th>
<th>100<del>240 VAC, 50</del>60 Hz, 1.2 A</th>
<th>100<del>240 VAC, 50</del>60 Hz, 1.2 A</th>
<th>100<del>240 VAC, 50</del>60 Hz, 1.2 A</th>
</tr>
</thead>
</table>

### Dimensions

<table>
<thead>
<tr>
<th>Dimensions (W) x (D) x (H) mm</th>
<th>216 x 140 x 33</th>
<th>216 x 140 x 33</th>
<th>242 x 167 x 35.5</th>
<th>242 x 175 x 35.5</th>
</tr>
</thead>
</table>

### Weight, kg

<table>
<thead>
<tr>
<th>Model</th>
<th>0.42</th>
<th>0.42</th>
<th>1.2</th>
<th>1.2</th>
</tr>
</thead>
</table>

### Notes

- * Testing Methods/Tests: Maximum performance based on RFC 2464 (UDP packets): 1,544 bytes. Actual performance may vary depending on network conditions and activated services
- *2 VPN Throughput measured using Iperf tool with a 1,544 bytes packet size based on RFC 2464
- *3 UTM Throughput measured using industry standard benchmark test tool against HTTP protocol with 1,544 bytes packet size. Testing done with multiple flows.
- *4 With SPI Firewall/UTM performance
- *5 With SSL/CAM module
- *6 More sessions measured using industry-standard benchmark test tool
Features

**Firewall**
- ICSA-certified firewall
- Routing and transparent (bridge) mode
- Zone-based access control list
- Stateful packet inspection
- NAT/PAT
- Policy base NAT
- VLAN tagging
- User-aware policy enforcement
- SIP/SSH NAT traversal
- ALG supports custom ports

**Virtual Private Network (VPN)**
- IKEv2/IPSec
- PPP/PPPv2/PPPoE
- Algorithm: AES/DES/3DES
- Authentication: SHA-1/MD5
- Key management: Manual key/IKE
- Perfect forward secrecy (DH groups) support
- Supports two-factor authentication
- Reverse proxy mode and full tunnel
- Clientless secure remote access
- VPN HA (redundant remote VPN gateways)
- Auto reconnect VPN
-强制用户身份认证（透明模式)
- Xauth over RADIUS for IPSec VPN
- External LDAP/RADIUS user database
- Local user database
- Maximum bandwidth
- Per host session limit
- DHCP client/server/relay
- Tagged VLAN (802.1Q)
- Layer 2 port grouping

**Anti-Virus (except USG 20/20W)**
- Support Kaspersky and ZyXEL Anti-Virus
- Stream-based Anti-Virus engine
- Zone base AV protection
- HTTP/FTP/SMTTP/POP3/IMAP4 protocol support
- Automatic signature updates
- No file size limitation
- Blacklist/whitelist support

**Application Patrol**
- Application, IM/IMP/2P, stream media, IP/IM media access control
- Deep packet inspection of IM (chat, file transfer, video)
- Application and IM/IMP/2P bandwidth control
- User authentication support
- IM/IMP signature auto update
- Support more than 15 catalogs IM and P2P
- Real-Time statistical reports
- Maximum/guaranteed bandwidth

**SSL VPN**
- Clientless secure remote access
- Support reverse proxy mode and full tunnel mode
- Unified policy enforcement
- Supports two-factor authentication
- Customizable user portal

**Intrusion Detection and Prevention (IDP) (except USG 50/20/20W)**
- Routing and transparent (bridge) mode
- Zone-based IDP inspection
- Customizable protection profile
- Protect over 2000 attack
- Automatic signature updates
- Custom signature
- Protocol anomaly detection and protection
- Traffic anomaly detection and protection
- Flooding detection and protection
- DoS/DDoS protection

**Content Filtering**
- Social networking control
- Web security—ZyXEL safe browsing
- URL blocking, keyword blocking
- Profile base setting
- Exempt list (blacklist and whitelist)
- Blocks java applet, cookies and active X
- Dynamic URL filtering database (powered by BlueCoast)
- Unlimited user licenses support
- Customizable warning messages and redirect URL

**Networking**
- Routing mode/bridge mode/mixed mode
- Layer 2 port grouping
- Ethernet/PPPv2
- Tagged VLAN (802.1Q)
- Virtual interface (alias interface)
- Policy-based routing (user-aware)
- Policy-based NAT (SNAT)
- Dynamic routing (RIP v1/v2, OSPF)
- DHCP client/server relay
- Dynamic DNS support
- WAN Trunk more than 2 port
- Per host session limit
- Guaranteed bandwidth
- Maximum bandwidth
- Priority/bandwidth utilization

**System Management**
- Role-based administration
- Multiple administrator login
- Multi-Lingual web GUI (HTTP/HTTPS)
- Out-of-band management (AX)
- Object-based configuration
- Command line interface (console/web console/webSSH/TELNET)
- SNMP v1/v2c

**E-Mail Filtering**
- LMTP/SMTP, POP3, IMAP4, MAPI, MIME, Outlook, MSN
- Maximum/guaranteed bandwidth
- Per host session limit
- DHCP client/server/relay
- Tagged VLAN (802.1Q)
- Layer 2 port grouping

**Accessories**

1. **Security Extension Module (USG 2000 only)**
   - SEM-DUAL
   - SEM-VPN
   - Product Photo
   - Features
   - For customers require full security features both VPN and UTM threat protections. The SEM-DUAL unleashes full horsepower of the ZyWALL USG 2000 platform with mighty VPN and UTM performance.
   - Secure ISAKMP 3001 for UTM Acceleration (Anti-Virus and IDP)
   - Advanced VPN Crypto to Boost up VPN Performance

2. **System Performance**
   - VPN Throughput (AES)\(^{2}\) 400 Mbps
   - UTM Throughput (AV+IDP)\(^{2}\) 400 Mbps
   - Max. IPSec VPN Tunnels 2,000
   - Max SSL VPN Users 750
   - Environmental Specifications
   - Operating Temperature 0°C to 40°C
   - Storage Temperature -20°C to 80°C
   - Operating Humidity 5% to 95% (non-condensing)
   - Physical Specifications
   - Dimensions, (WxixDxH) (mm) 199 x 212 x 36.3
   - Weight (G) 410

Note:
- \(^{2}\) UTM AV/IDS throughputs measured using industry standard baselines and test tool against.

**Transceiver**

- **Model Name**
- **Connector**
- **Wavelength**
- **Max Transmission Distance**
- **Optical Budget**
- **Laser Transmitter Characteristics**
- **Maximum Launch Power**
- **Minimum Launch Power**
- **Maximum Input Power**
- **Receivers Characteristics**

- **SFP-5X-D**
  - LC
  - 850 nm
  - 550 m
  - 7.5 dB
  - -4 dBm
  - -0.5 dBm
  - -17 dBm

- **SFP-10X-D**
  - LC
  - 1310 nm
  - 10 km
  - 10.5 dB
  - -3 dBm
  - -0.5 dBm
  - -20 dBm

- **SFP-LH1510-40-D**
  - LC
  - 1310 nm
  - 40 km
  - 21 dB
  - +3 dBm
  - -23 dBm

- **SFP-ZX-80-D**
  - LC
  - 1550 nm
  - 80 km
  - 24 dB
  - +5 dBm
  - -24 dBm

*Note: *SFP-5X-D, SFP-10X-D, SFP-LH1510-40-D, SFP-ZX-80-D are designed for use with ZyXEL internal products only.*