



# Your PDF Guides

You can read the recommendations in the user guide, the technical guide or the installation guide for ZYXEL ZYWALL USG 20W. You'll find the answers to all your questions on the ZYXEL ZYWALL USG 20W in the user manual (information, specifications, safety advice, size, accessories, etc.). Detailed instructions for use are in the User's Guide.

**User manual ZYXEL ZYWALL USG 20W**  
**User guide ZYXEL ZYWALL USG 20W**  
**Operating instructions ZYXEL ZYWALL USG 20W**  
**Instructions for use ZYXEL ZYWALL USG 20W**  
**Instruction manual ZYXEL ZYWALL USG 20W**



**ZyWALL USG 20/  
20W/50/100/200/  
300/1000/2000**  
Unified Security Gateway

**Security Licenses**

Product	Duration	ZyXEL Anti-Virus	Essentially Anti-Virus	IDP	Content Filter	Usage CDM	Warranty Report
USG 2000	1 year	Yes	Yes	Yes	Yes	All ZyWALL models support: 1 device 5 devices 25 devices 100 devices 300 devices 1000 nodes	
	2 years	Yes	Yes	Yes	Yes		
USG 1000	1 year	Yes	Yes	Yes	Yes		
	2 years	Yes	Yes	Yes	Yes		
USG 300	1 year	Yes	Yes	Yes	Yes		
	2 years	Yes	Yes	Yes	Yes		
USG 200	1 year	Yes	Yes	Yes	Yes		
	2 years	Yes	Yes	Yes	Yes		
USG 100	1 year	Yes	Yes	Yes	Yes		
	2 years	Yes	Yes	Yes	Yes		
USG 50	1 year	-	-	-	Yes		
	2 years	-	-	-	Yes		
USG 20	1 year	-	-	-	Yes		
	2 years	-	-	-	Yes		

  

Product	SSL VPN	IPSec VPN Clients
USG 2000	510-30 SSL Tunnels	For Client PCs Software client 1 license Software client 50 licenses Software client 500 licenses
	510-250 SSL Tunnels	
	510-750 SSL Tunnels	
	5010-290 SSL Tunnels	
	25010-750 SSL Tunnels	
USG 1000	510-25 SSL Tunnels	For Client PCs Software client 1 license Software client 10 licenses Software client 50 licenses
	510-10 SSL Tunnels	
	510-250 SSL Tunnels	
	2510-290 SSL Tunnels	
	10100-290 SSL Tunnels	
USG 300	210-25 SSL Tunnels	For Client PCs Software client 1 license Software client 10 licenses Software client 50 licenses
	1010-25 SSL Tunnels	
USG 200	210-10 SSL Tunnels	For Client PCs Software client 1 license Software client 10 licenses Software client 50 licenses
USG 100	210-5 SSL Tunnels	
USG 50	210-5 SSL Tunnels	For Client PCs Software client 1 license Software client 10 licenses Software client 50 licenses
USG 20	-	
USG 20W	-	

**3G Card Support**

Please visit [http://www.zyxel.com/products\\_services/usb\\_security.html](http://www.zyxel.com/products_services/usb_security.html) and find the following path:  
ZyWALL Unified Security Gateways → USG product pages to see the 3G Card Compatibility list for supported USB devices.

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

Copyright © 2011 ZyXEL Communications Corp. All rights reserved. ZyXEL, ZyWALL and Unified Security Gateway are registered trademarks of ZyXEL Communications Corp. All other marks are the property of their respective owners. All other trademarks are the property of their respective owners.




**Unified Security Gateway for Small and Medium-sized Companies**

The ZyWALL USG (Unified Security Gateway) Series is the "third generation" ZyWALL featuring an all-new platform. It provides greater performance protection, as well as a deep packet inspection security solution for small businesses to enterprises alike. It embodies a Stateful Packet Inspection (SPI) Firewall, Anti-Virus (AV), Intrusion Detection and Prevention (IDP), Content Filtering, Anti-Spam, and VPN (IPSec/SSL/2TP) in one box. This multi-layered security safeguards your organization's customer and company records, intellectual property, and critical resources from external and internal threats.

**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 more and more valuable information. The infrastructure should be tailored to meet operation requirements for expanding remote sites as well as mobile teleworkers.
- Proactive protection**  
The evolving Web environment not only makes managing appropriate surfing and bandwidth use more difficult, but also introduces new security threats for the filtering functionality to prevent on. The ZyWALL USG Content Filter leverages the next-generation Web filtering technology by combining URL, Filtering and anti-malware technologies into a collaborative cloud defense architecture powered by BlackICE, which is capable of protecting user products by while blocking malware download and Web threats.
- 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 cause legal hassles.
- 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 build up a highly available network infrastructure for non-stop operations.
- Manageability**  
With ZyWALL USG and Manage-CNM (Centralized Network Management), users can achieve the following objects to reduce operational costs:
  - Easy VPN management and diagnostic capability
  - Complete security policies and UTM management
  - Active monitoring, alerting and comprehensive graphic reports

**ZyWALL USG 20/  
20W/50/100/200/  
300/1000/2000**  
Unified Security Gateway



[You're reading an excerpt. Click here to read official ZYXEL ZYWALL USG 20W user guide](http://yourpdfguides.com/dref/4124640)  
<http://yourpdfguides.com/dref/4124640>

**Manual abstract:**

It provides greater performance protection, as well as a deep packet inspection security solution for small businesses to enterprises alike. It embodies a Stateful Packet Inspection (SPI) Firewall, Anti-Virus (AV), Intrusion Detection and Prevention (IDP), Content Filtering, Anti-Spam, and VPN (IPSec/SSL/L2TP) in one box. @@@@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 hassles. 3G Card Support Please visit [http://www.zyxel.com/products\\_services/smb\\_security.shtml](http://www.zyxel.com/products_services/smb_security.shtml) and find the following path: ZyWALL Unified Security Gateways USG product pages to see the 3G Card Compatibility List for supported USB devices. 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 build up a highly available network infrastructure for non-stop operations. For more product information, visit us on the web at www.

ZyXEL . com Copyright © 2011 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. 5-100-00811002 06/11 ZyWALL USG 20/ 20W/50/100/200/ 300/1000/2000 Unified Security Gateway Manageability With ZyWALL USG and Vantage CNM (Centralized Network Management), users can achieve the following objects to reduce operational costs: · Easy VPN management and diagnostic capability · Complete security policies and UTM management · Active monitoring, alerting and comprehensive graphic reports ZyWALL USG 20/ 20W/50/100/200/ 300/1000/2000 Unified Security Gateway 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. Stateful Firewall Anomaly Detection and Prevention (PA/TA) Application Classifier Traffic Out Traffic In Endpoint security Network g I/O Engine Defragment DNAT Forwarding Engine Routing SNAT BWM Network I/O Engine Fragment With the new Endpoint Security (EPS) feature, administrators can easily identify policy-violating users such as those who don't have AV software installed. With additional AV software installed, the ZyWALL can help mitigate virus threats and therefore prevent the loss of money and employee productivity. The EPS supports Norton™, Kaspersky™, TrendMicro™ AV client software and many others. Moreover, the new EPS feature also supports personal LAN User 1 LAN User 2 LAN Checking 1. Anti-Virus 2. Personal Firewall 3. OS patch level The result is NO Access Checking 1. Anti-Virus 2. Personal Firewall 3. OS patch level The result is Access DMZ (Server Farm) Email Server BI System Web-based Application LAN Application Server OA, ERP System (Inventory, Store...

) CRM System Remote Desktop SSL-VPN User Threat Database Update Intrusion Detection and Prevention Anti-Virus Application Patrol Content Filter Anti-Spam Clean Traffic firewall software such as Kaspersky Internet Security 2009/2010, Windows Firewall and TrendMicro PC-Cillin/Internet Security 2010. Checking 1. Anti-Virus 2. Personal Firewall 3. @@@@Take the USG 50 as an example: its excellent performance Business Related Applications Allow Business Related Non-Business Related Applications Bandwidth Limit IM P2P Block 0 ZyWALL 5 FG-30B TZ100 ZyWALL USG 50 0 ZyWALL 5 FG-30B TZ100 ZyWALL USG 50 25 2500 50 5000 75 7500 100 Competitive Comparison: Firewall Throughput in Mbps 10000 Competitive Comparison: Sessions delivers sufficient speed boost to meet all small business needs. \* Source: Performance figures from ZyXEL, SonicWALL and Fortinet Websites. 4 5 ZyWALL USG 20/ 20W/50/100/200/ 300/1000/2000 Unified Security Gateway High Availability (HA) HA is essential to enterprise networks. It ensures a system or a component to remain continuously operational for a reasonable, desirable period. The ZyWALL USG Series provides HA features such as: · Multiple WAN ports and configurable load balancing between ports. · An auxiliary (backup) Internet connection known as out-of-band management. · A backup ZyWALL in case the master ZyWALL fails (Device HA). To minimize the impact of single-point failures, the ZyWALL USG Series supports Device HA to ensure network availability. PWR Non-stop Internet access with Devicenterface 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 SB (1~10 PC Users) · All Gigabit Ethernet interface hardware design · High-performance multi-layer threat protection · Hybrid VPN (IPSec, SSL) secures connection · Multi WAN ports for multiple ISP links and load balancing · Unified Security Gateway for SMB (10~25 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 (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 · Flexible OPT (option) port · Unified Security Gateway for SMB (50~75 PC Users) · Providing Hybrid VPN (IPSec/SSL VPN) and robust UTM security services · High-performance multi-layer threat protection · User-aware policy engine enables access granularity · Excellent manageability with object, text-based and centralized management · Unified Security Gateway for SMB (75~200 PC Users) · Providing Hybrid VPN (IPSec/SSL VPN) and robust UTM security services · High-performance multi-layer threat protection · Non-stop operations of mission-critical applications · Excellent manageability with object, text-based and centralized management · Unified Security Gateway for SMB (200~500 PC Users) · Gigabit Firewall with Fiber interface (SFP) · Scalable VPN/UTM performance · Support Kaspersky and ZyXEL Anti-Virus · Redundant power module Hardware Specifications 10/100/1000 Interfaces (Copper) Dual Personality GbE (SFP/RJ45) USB Ports SEM Slot (Security Extension Module) Card Slot 802.



[You're reading an excerpt. Click here to read official ZYXEL ZYWALL USG 20W user guide](#)  
<http://yourpdfguides.com/dref/4124640>

11b/g/n 2x2 Antenna System Capacity & Performance SPI Firewall Throughput\*1 (Mbps) VPN Throughput (AES)\*2 (Mbps) UTM Throughput (AV+IDP)\*3 (Mbps) Wi-Fi Throughput\*4 (Mbps) Unlimited User Licenses Max. Sessions\*5 New Session Rate Max.

Concurrent IPsec VPN Tunnels Max. Concurrent SSL VPN Users Included SSL VPN Users Customizable Zone Power Requirement Input Voltage Power Rating Physical Specifications Item dimensions (W x D x H)(mm/in.) Item weight (kg/lb.) Packing dimensions (W x D x H)(mm/in.) Packing weight (kg/lb.) Environmental Specifications Operating temperature Storage temperature Operating humidity 0°C to 40°C/32°F to 104°F -30°C to 60°C/-22°F to 140°F 5% to 90% (Non-condensing) 0°C to 40°C/32°F to 104°F -30°C to 60°C/-22°F to 140°F 5% to 90% (Non-condensing) 0°C to 40°C/32°F to 104°F -30°C to 60°C/-22°F to 140°F 5% to 90% (Non-condensing) 0°C to 40°C/32°F to 104°F -30°C to 60°C/-22°F to 140°F 5% to 90% (Non-condensing) 0°C to 40°C/32°F to 104°F -30°C to 60°C/-22°F to 140°F 5% to 90% (Non-condensing) 0°C to 40°C/32°F to 104°F -30°C to 60°C/-22°F to 140°F 5% to 90% (Non-condensing) 0°C to 40°C/32°F to 104°F -30°C to 60°C/-22°F to 140°F 5% to 90% (Non-condensing) 0°C to 40°C/32°F to 104°F -30°C to 60°C/-22°F to 140°F 5% to 90% (Non-condensing) 216 x 140 x 33/ 8.50 x 5.51 x 1.30 0.42/0.93 305 x 205 x 106/ 12.01 x 8.07 x 4.17 1.1/2.

43 216 x 140 x 33/ 8.50 x 5.51 x 1.30 0.38/0.84 305 x 205 x 106/ 12.01 x 8.07 x 4.17 1/2.20 242 x 167 x 35.  
5/ 9.53 x 6.57 x 1.40 1.2/2.

65 375 x 238 x 108/ 14.76 x 9.37 x 4.25 2.4/5.

29 242 x 175 x 35.5/ 9.53 x 6.89 x 1.40 1.2/2.65 296 x 158 x 241/ 11.65 x 6.22 x 9.49 2.

7/5.95 242 x 175 x 35.5/ 9.53 x 6.89 x 1.40 1.2/2.65 296 x 158 x 241/ 11.65 x 6.22 x 9.

49 3/6.61 430 x 201 x 42/ 16.93 x 7.91 x 1.65 2.

8/6.17 539 x 184 x 321/ 21.22 x 7.24 x 12.64 6/13.

22 431 x 292 x 43.5/ 16.97 x 11.50 x 1.71 4.7/10.36 529 x 411 x 194/ 20.83 x 16.18 x 7.64 6.

5/14.33 430 x 487 x 89/ 16.93 x 19.17 x 3.50 10.5/23.15 607 x 551 x 295/ 23.90 x 21.70 x 11.61 14.

2/31.31 100 - 240 V AC, 50 - 60 Hz, 1.2 A 16 W Max 100 - 240 V AC, 50 - 60 Hz, 1.2 A 15 W Max 100 - 240 V AC, 50 - 60 Hz, 1.2 A 17 W Max 100 - 240 V AC, 50 - 60 Hz, 1.

2 A 20 W Max 100 - 240 V AC, 50 - 60 Hz, 1.2 A 20 W Max 100 - 240 V AC, 50/60 Hz, 0.55 - 0.3 A 35 W Max 100 - 240 V AC, 50/60 Hz, 1 A Max 80 W Max 100 - 240 V AC, 50 - 60 Hz, 3 - 6 A 200 W Max 150 75 80 Yes 6,000 900 5 1 1 Yes 150 75 Yes 6,000 900 5 1 1 Yes 180 90 24 Yes 10,000 1,000 5 5 2 Yes 180 90 30 Yes 20,000 1,000 50 5 2 Yes 250 90 40 Yes 40,000 1,000 100 10 2 Yes 300 130 80 Yes 60,000 1,500 200 25 2 Yes 400 180 100 Yes 500,000 12,000 1,000 250 5 Yes 2,000 600\*6 400\*7 Yes 1,000,000 20,000 2,000 750\*6 5 Yes 4 x LAN/DMZ, 1 x WAN 1 Yes Yes 4 x LAN/DMZ, 1 x WAN 1 4 x LAN/DMZ, 2 x WAN 2 5 x LAN/DMZ, 2 x WAN 2 1 5 x LAN/DMZ, 2 x WAN, 1 x OPT 2 1 7 2 2 5 2 1 6 2 2 1 1 - Note: Actual performance may vary depending on network conditions and activated services. \*1: Testing Methodologies: Maximum performance based on RFC 2544 (UDP packets, 1,518 bytes).

\*2: VPN (AES) throughput measured using UDP traffic with 1,424 bytes packet size, based on RFC 2544. \*3: UTM (AV+IDP) throughput measured using industry standard IXIA IxLoad test tool against HTTP protocol with 1,460 bytes packet size. Testing done with multiple flows. \*4: 11n (20 MHz), security type: WPA2-PSK \*5: Max sessions measured using industry standard IXIA IxLoad test tool. @@@@ @@@@. SecuASIC CIP-3001 for UTM acceleration (Anti-Virus and IDP) · Advanced VPN Crypto to boost VPN performance 600 400 2,000 750 600 100 2,000 750 Anti-Spam · Zone to zone protection · Transparently intercept mail via SMTP/POP3 protocols · Blacklist/whitelist support · Support DNSBL checking · Spam tag support · Statistics report Authentication · Local user database · Microsoft Windows active directory integrate · External LDAP/RADIUS user database · Xauth over RADIUS for IPsec VPN · Forced user authentication (transparent authentication) · IP/MAC address binding SSL VPN · Clientless secure remote access · Support reverse proxy mode and full tunnel mode · Unified policy enforcement · Supports two-factor authentication · Customizable user portal High Availability (except USG 50/20/20W) · Active-Passive mode · Device failure detection and notification · Support ICMP and TCP ping check · Link monitoring · Auto-Sync configurations System Management · Role-Based administration · Multiple administrator login · Multi-Lingual web GUI (HTTPS/HTTP) · Object-based configuration · Command line interface (console/web console/SSH/TELNET) · SNMP v2c (MIB-II) · System configuration rollback · Firmware upgrade via FTP/FTP-TLS/web GUI

Note: \*8: VPN (AES) HTTP protocol with 1,460 bytes packet size. Testing done with multiple flows. \*9: UTM (AV+IDP) throughput measured using industry standard IXIA IxLoad test tool against. Transceiver Model Name SFP-SX-D SFP-LX-10-D SFP-LHX1310-40-D SFP-ZX-80-D Connector LC LC LC LC LC Wavelength 850 nm 1310 nm 1310 nm 1550 nm Max Transmission Distance 550 m 10 km 40 km 80 km Laser Transmitter Characteristics Optical Budget 7.5 dB 10.5 dB 21 dB 24 dB Maximum Launch Power -4 dBm -3 dBm +3 dBm +5 dBm Minimum Launch Power -9.

5 dBm -9.5 dBm -2 dBm 0 dBm Receiver Characteristics Optical Receiver Sensibility -17 dBm -20 dBm -23 dBm -24 dBm Maximum Input Power -3 dBm -3 dBm -3 dBm -3 dBm Intrusion Detection and Prevention (IDP)(except USG 20/20W) · Routing and transparent (bridge) mode · Zone-based IDP inspection · Customizable protection profile · Protect over 2000 attack · Automatic signature updates · Custom signatures · Protocol anomaly detection and protection · Traffic anomaly detection and protection · Flooding detection and protection · DoS/DDoS protection Content Filtering · Social networking control · Web security--Security threat category (powered by BlueCoat) · 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 BlueCoat) · Unlimited user licenses support · Customize warning messages and redirect URL Logging/Monitoring · Comprehensive local logging · Syslog (send to up to 4 servers) · E-mail alert (send to up to 2 servers) · Real-Time traffic monitoring · Built-in daily report · Advanced reporting (Vantage Report) · Centralized Network Management (Vantage CNM) manageable 802.11b 802.



[You're reading an excerpt. Click here to read official ZYXEL ZYWALL USG 20W user guide](http://yourpdfguides.com/dref/4124640)  
<http://yourpdfguides.com/dref/4124640>

11g 802.11n Model Maximum Output Power 802.11b 802.11g 802.11n 11 Mbps 54 Mbps 20 MHz 40 MHz 11 Mbps 54 Mbps 20 MHz 40 MHz 18.5 dBm 15.5 dBm 15.

5 dBm 12.5 dBm -83 dBm -70 dBm -64 dBm -61 dBm USG 20W Wireless Radio Information (USG 20W) Anti-Virus (except USG 20/20W) · Support Kaspersky and ZyXEL Anti-Virus · Stream-based Anti-Virus engine Radio Sensitivity 10 11 .



[You're reading an excerpt. Click here to read official ZYXEL ZYWALL USG 20W user guide](#)  
<http://yourpdfguides.com/dref/4124640>