ZyXEL

Security Licenses

Product	Duration	ZyXEL Anti-Virus	Kaspersky Anti-Virus	IDP	Content Filter	Vantage CNM	Vantage Report
USG 2000	1 year	Yes	Yes	Yes	Yes		
	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	All ZyWALL models support:	All ZyWALL models support:
	2 years	Yes	Yes	Yes	Yes	10 nodes	1 device
USG 200	1 year	Yes	Yes	Yes	Yes	25 nodes	5 devices
	2 years	Yes	Yes	Yes	Yes	50 nodes	25 devices
USG 100	1 year	Yes	Yes	Yes	Yes	100 nodes	100 devices
	2 years	Yes	Yes	Yes	Yes	300 nodes	
USG 50	1 year	Yes	Yes	Yes	Yes	1000 nodes	
	2 years	Yes	Yes	Yes	Yes		
USG 20	1 year	-	-	-	Yes		
	2 years	-	-	-	Yes		
USG 20W	1 year	-	-	-	Yes		
	2 years	-	-	-	Yes		

Product	SSL VPN	IPSec VPN Client
USG 2000	5 to 50 SSL Tunnels	
	5 to 250 SSL Tunnels	
	5 to 750 SSL Tunnels	
	50 to 250 SSL Tunnels	
	50 to 750 SSL Tunnels	
	250 to 750 SSL Tunnels	
USG 1000	5 to 25 SSL Tunnels	For Client PC's
	5 to 50 SSL Tunnels	Software client 1 license
	5 to 250 SSL Tunnels	Software client 5 licenses
	25 to 50 SSL Tunnels	Software client 10 licenses
	25 to 250 SSL Tunnels	Software client 50 licenses
	50 to 250 SSL Tunnels	
USG 300	2 to 10 SSL Tunnels	
	2 to 25 SSL Tunnels	
	10 to 25 SSL Tunnels	
USG 200	2 to 10 SSL Tunnels	
USG 100	2 to 5 SSL Tunnels	
USG 50	2 to 5 SSL Tunnels	
USG 20	-	
USG 20W	-	

3G Card Support

Please visit **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.

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

5-100-00811002   06/11

ZyXEL

- **All-new platform: "3rd" generation ZyWALL**
- **USG clean-traffic architecture**
- **New generation UTM solution (except USG 20/20W)**
- **Robust hybrid VPN (IPSec and SSL)**
- **Content filter stops malware and Web threats**
- **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**
- **ZyXEL Security Distribution Network (ZSDN)**

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/L2TP) in one box. This multilayered 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 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

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 pinpoint 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 BlueCoat, which is capable of protecting user productivity while blocking malware downloads 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 create 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 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
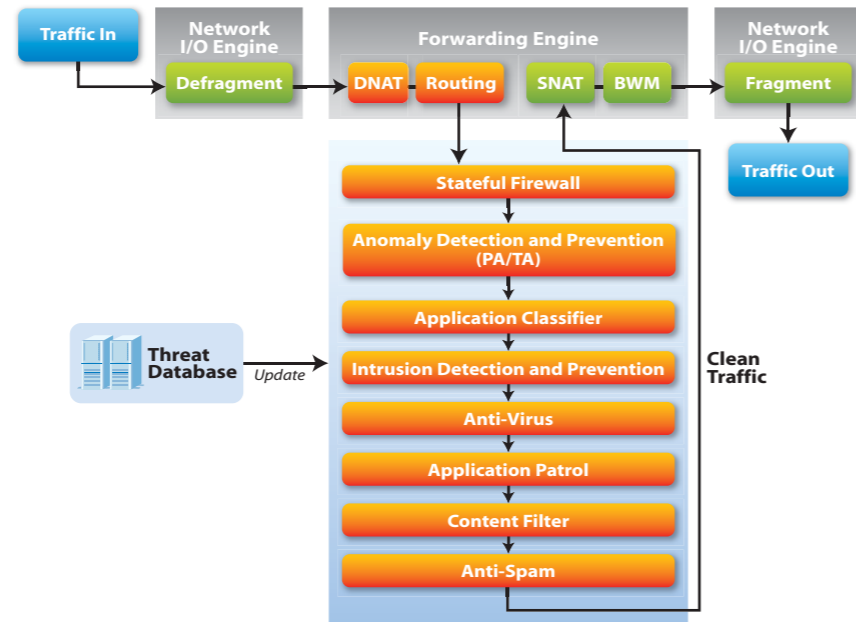- Active monitoring, alerting and comprehensive graphic reports

ZyXEL

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

Key Applications

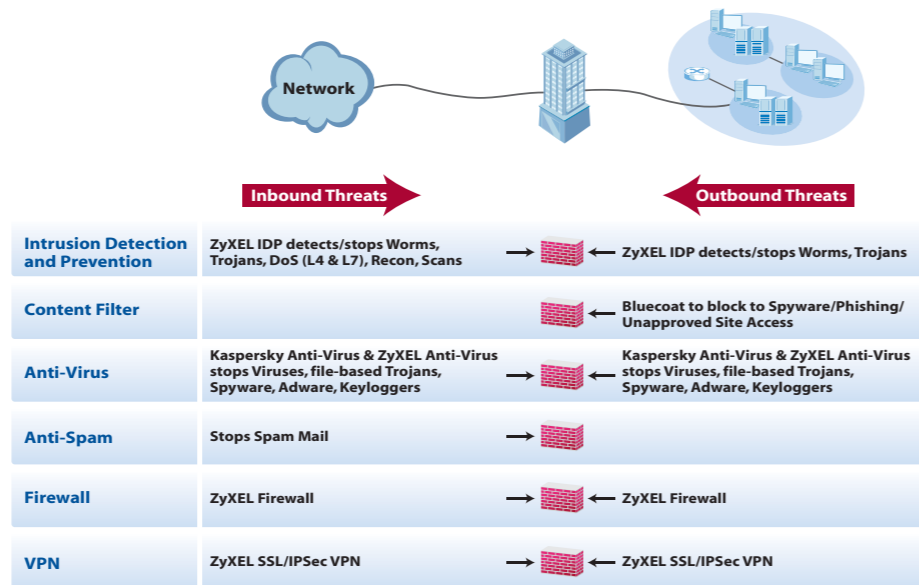### ZyWALL USG clean-traffic architecture

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.
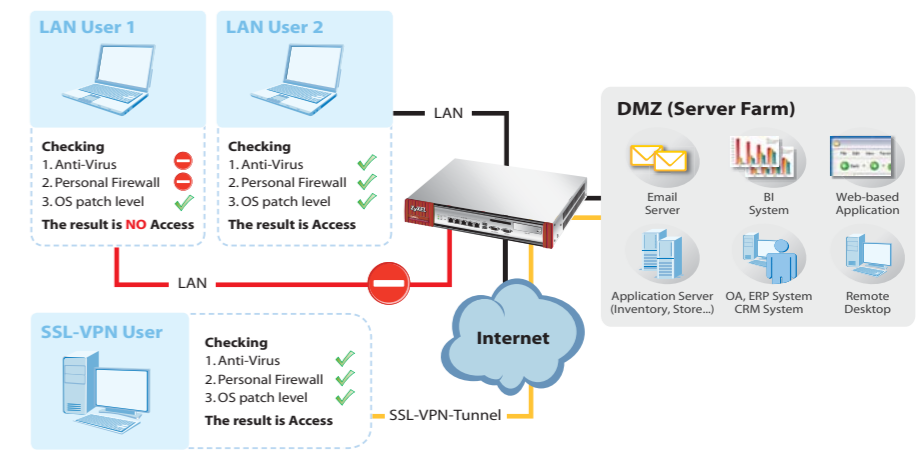
Traffic In

Network I/O Engine
- Defragment

Forwarding Engine
- DNAT
- Routing
- SNAT
- BWM

Network I/O Engine
- Fragment

Traffic Out

- Stateful Firewall
- Anomaly Detection and Prevention (PA/TA)
- Application Classifier
- Intrusion Detection and Prevention
- Anti-Virus
- Application Patrol
- Content Filter
- Anti-Spam

Threat Database — *Update*

Clean Traffic

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, VPN. All ZyWALL USG Series products support the Gigabit Ethernet.

Network

Inbound Threats ← → **Outbound Threats**

	Inbound Threats	Outbound Threats
Intrusion Detection and Prevention	ZyXEL IDP detects/stops Worms, Trojans, DoS (L4 & L7), Recon, Scans	ZyXEL IDP detects/stops Worms, Trojans
Content Filter		Bluecoat to block to Spyware/Phishing/Unapproved Site Access
Anti-Virus	Kaspersky Anti-Virus & ZyXEL Anti-Virus stops Viruses, file-based Trojans, Spyware, Adware, Keyloggers	Kaspersky Anti-Virus & ZyXEL Anti-Virus stops Viruses, file-based Trojans, Spyware, Adware, Keyloggers
Anti-Spam	Stops Spam Mail	
Firewall	ZyXEL Firewall	ZyXEL Firewall
VPN	ZyXEL SSL/IPSec VPN	ZyXEL SSL/IPSec VPN

ZyXEL

Endpoint security

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 firewall software such as Kaspersky Internet Security 2009/2010, Windows Firewall and TrendMicro PC-Cillin/Internet Security 2010.

LAN User 1
Checking
1. Anti-Virus
2. Personal Firewall
3. OS patch level
The result is NO Access

LAN User 2
Checking
1. Anti-Virus
2. Personal Firewall
3. OS patch level
The result is Access

SSL-VPN User
Checking
1. Anti-Virus
2. Personal Firewall
3. OS patch level
The result is Access

LAN

SSL-VPN-Tunnel

Internet

DMZ (Server Farm)
- Email Server
- BI System
- Web-based Application
- Application Server (Inventory, Store...)
- OA, ERP System CRM System
- Remote Desktop

* The USG's new EPS feature helps to ensure that all clients meet the corporate security policies; e.g. it checks if AV software is installed.

Content Filter stops malware and Web threats

The ZyWALL USG Content Filter enables businesses to protect their users and networks from malware and abuse such as spyware, phishing attacks and inappropriate P2P or IM usage. It keeps office computers from getting infected by dangerous malware and comprehensively protects business network environments.
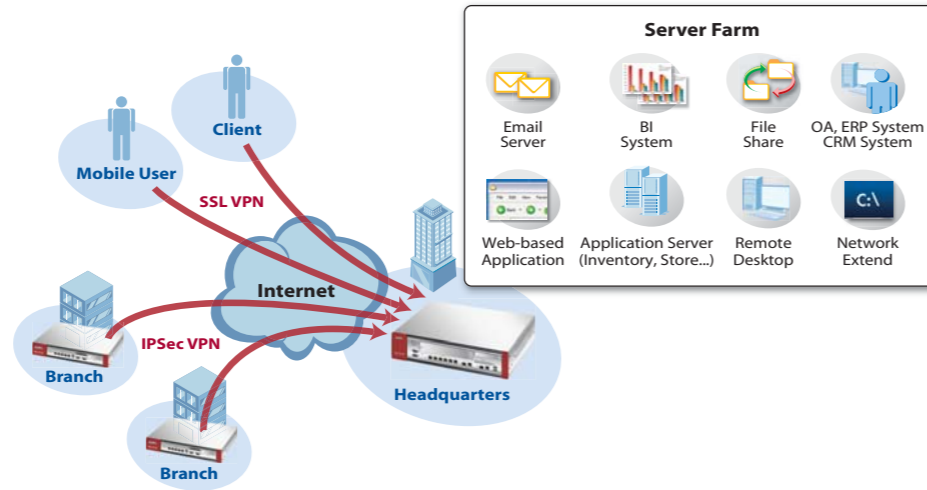
- P2P
- Virus
- IM
- Phishing
- Spyware

Blue Coat®
KASPERSKY

ZyXEL

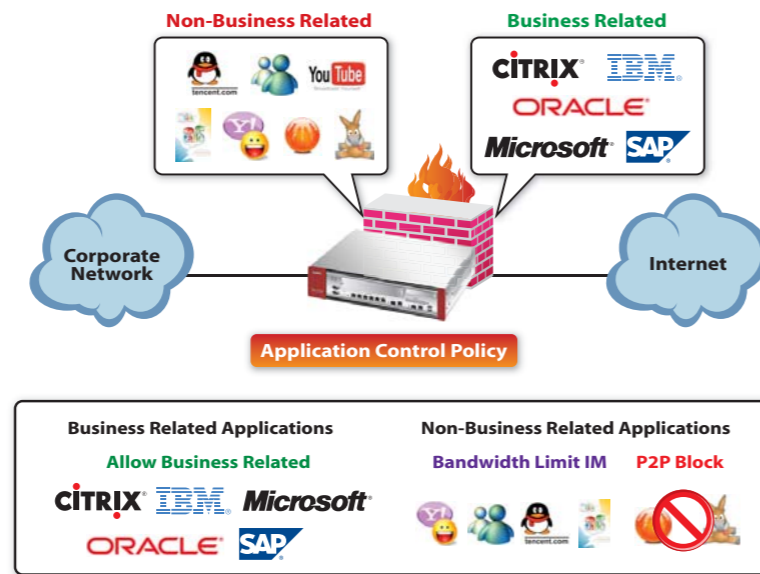## ZyWALL USG 20/20W/50/100/200/300/1000/2000
Unified Security Gateway

Robust hybrid VPN (IPSec and SSL)

The ZyWALL USG Series can provide secure access between remote locations and corporate resources through the Internet for organizations of any size. Using IPSec VPN, companies can secure connections to branch offices, partners and headquarters. Road warriors and telecommuters can use SSL or L2TP VPN to safely access the company network without having to install VPN software. The Series provides a flexible and easy way to enable mobile employees, vendors and partners to confidently access your network resource for better efficiency.

Server Farm

Email Server	BI System	File Share	OA, ERP System CRM System
Web-based Application	Application Server (Inventory, Store...)	Remote Desktop	Network Extend

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.


Non-Business Related   **Business Related**

Corporate Network   Internet

Application Control Policy

Business Related Applications	Non-Business Related Applications	
Allow Business Related	**Bandwidth Limit IM**	**P2P Block**

Granular control over social networking applications

Social networking applications such as Facebook, Twitter and YouTube have become an Internet phenomenon allowing people to quickly connect and share information with each other. However, social networking applications could eclipse business productivity considerably without flexible management. The ZyWALL USG Series prevents the Internet connection from being abused to minimize bandwidth waste or human resource policy violations. The ZyWALL USG Series provides granular control over the usage of social networking applications.

Without social network control   **With social network control**

Low Productivity   High Productivity
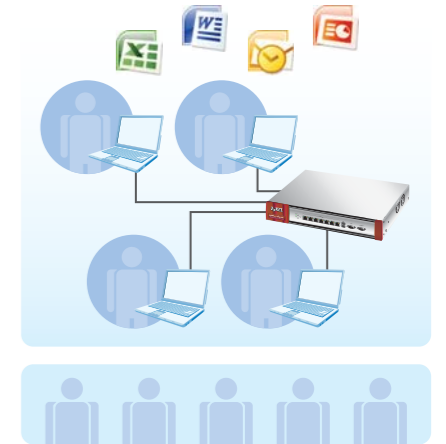
High performance

The ZyXEL USG Series is built with a powerful Integrated High Performance Security architecture, a proven architecture designed for ultrafast Gigabit fiber; it provides real-time inspection to prevent networks from threats without sacrificing performance. Corporate networks are not only flawlessly secured but also get significant performance enhancements on productivity and efficiency, since file loading, emailing and information searching applications are processed at higher speeds. Take the USG 50 as an example: its excellent performance delivers sufficient speed boost to meet all small business needs.

Competitive Comparison: Firewall Throughput in Mbps

Competitive Comparison: Sessions
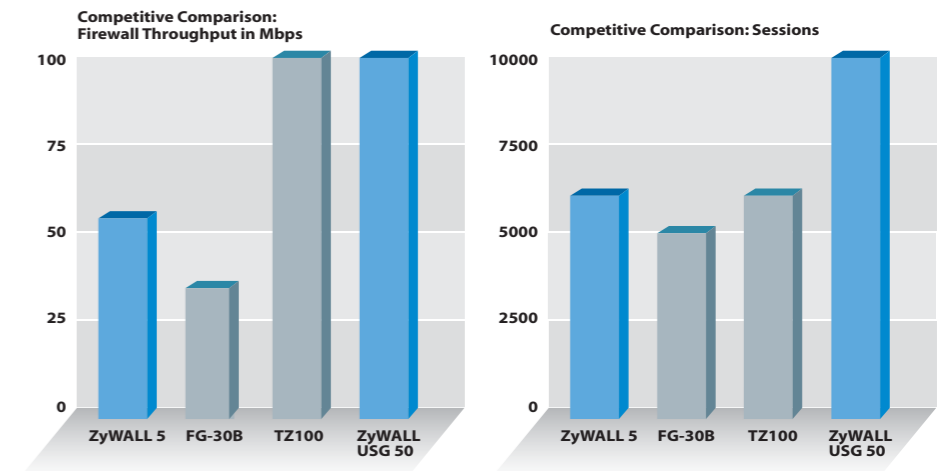
* Source: Performance figures from ZyXEL, SonicWALL and Fortinet Websites.

ZyXEL

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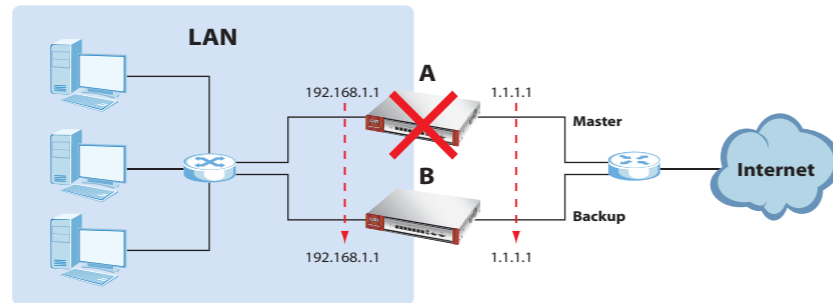
ZyXEL

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.

Device HA: Master Fails and Backup Takes Over

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.

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.

USG built-in reporting system

The ZyWALL USG Series provides a built-in reporting system to collect data and display various statistics of traffics passing through your ZyWALL.

Vantage Report: the centralized reporting system

Vantage Report is a cost-effective solution that allows administrators to easily monitor and analyze reports of ZyWALL USG Series from any location. It delivers statistical reports of rich formats for the IT staff to thoroughly control the bandwidth usage, security events and Web traffic analysis results.

Monitor
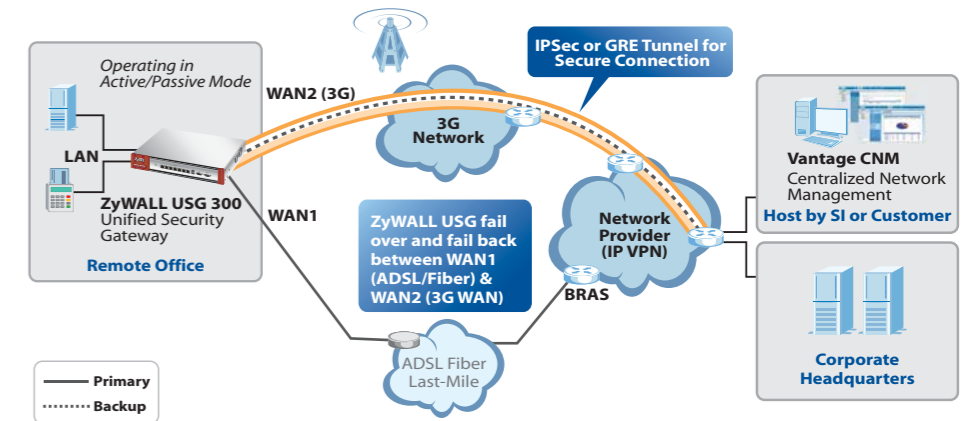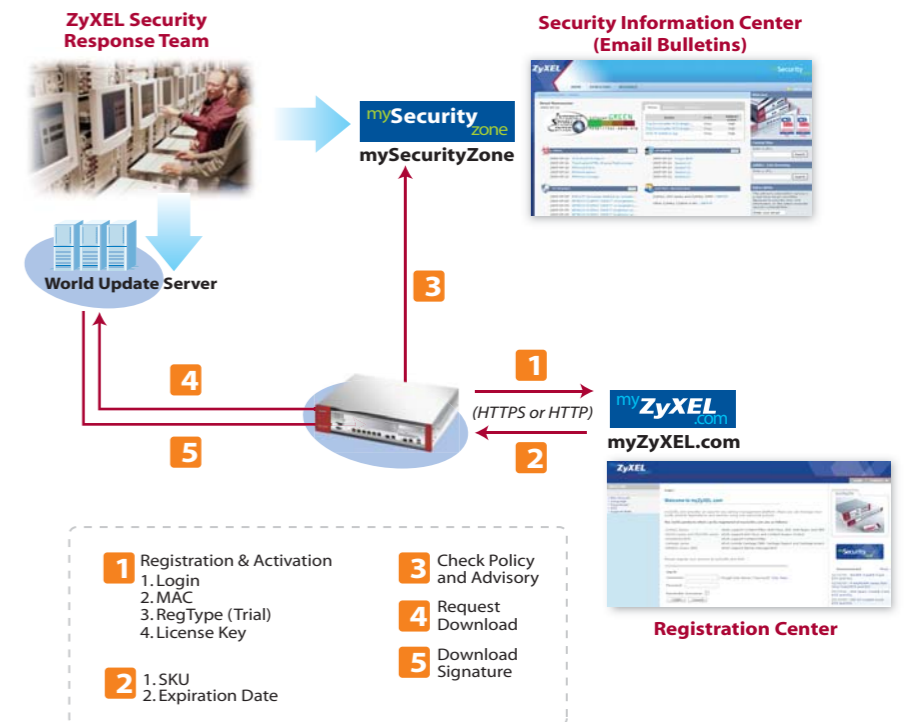

Statistical Report

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 Server 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.

1 Registration & Activation
1. Login
2. MAC
3. RegType (Trial)
4. License Key

2 1. SKU
2. Expiration Date

3 Check Policy and Advisory

4 Request Download

5 Download Signature

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

Specifications

Model	SB			SMB				
	ZyWALL USG 20W	ZyWALL USG 20	ZyWALL USG 50	ZyWALL USG 100	ZyWALL USG 200	ZyWALL USG 300	ZyWALL USG 1000	ZyWALL USG 2000
Product Photo								
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 • 802.11b/g/n wireless AP	• 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	• 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)	4 x LAN/DMZ, 1 x WAN	4 x LAN/DMZ, 1 x WAN	4 x LAN/DMZ, 2 x WAN	5 x LAN/DMZ, 2 x WAN	5 x LAN/DMZ, 2 x WAN, 1 x OPT	7	5	6
Dual Personality GbE (SFP/RJ45)	-	-	-	-	-	-	-	2
USB Ports	1	1	2	2	2	2	2	2
SEM Slot (Security Extension Module)	-	-	-	-	-	-	-	1
Card Slot	-	-	-	1	1	2	1	1
802.11b/g/n	Yes	-	-	-	-	-	-	-
2x2 Antenna	Yes	-	-	-	-	-	-	-
System Capacity & Performance								
SPI Firewall Throughput*1 (Mbps)	150	150	180	180	250	300	400	2,000
VPN Throughput (AES)*2 (Mbps)	75	75	90	90	90	130	180	600*6
UTM Throughput (AV+IDP)*3 (Mbps)	-	-	24	30	40	80	100	400*7
Wi-Fi Throughput*4 (Mbps)	80	-	-	-	-	-	-	-
Unlimited User Licenses	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Max. Sessions*5	6,000	6,000	10,000	20,000	40,000	60,000	500,000	1,000,000
New Session Rate	900	900	1,000	1,000	1,000	1,500	12,000	20,000
Max. Concurrent IPSec VPN Tunnels	5	5	5	50	100	200	1,000	2,000
Max. Concurrent SSL VPN Users	1	1	5	5	10	25	250	750*6
Included SSL VPN Users	1	1	2	2	2	2	5	5
Customizable Zone	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Power Requirement								
Input Voltage	100 - 240 V AC, 50 - 60 Hz, 1.2 A	100 - 240 V AC, 50 - 60 Hz, 1.2 A	100 - 240 V AC, 50 - 60 Hz, 1.2 A	100 - 240 V AC, 50 - 60 Hz, 1.2 A	100 - 240 V AC, 50 - 60 Hz, 1.2 A	100 - 240 V AC, 50/60 Hz, 0.55 - 0.3 A	100 - 240 V AC, 50/60 Hz, 1 A Max	100 - 240 V AC, 50 - 60 Hz, 3 - 6 A
Power Rating	16 W Max	15 W Max	17 W Max	20 W Max	20 W Max	35 W Max	80 W Max	200 W Max
Physical Specifications								
Item dimensions (W x D x H)(mm/in.)	216 x 140 x 33/ 8.50 x 5.51 x 1.30	216 x 140 x 33/ 8.50 x 5.51 x 1.30	242 x 167 x 35.5/ 9.53 x 6.57 x 1.40	242 x 175 x 35.5/ 9.53 x 6.89 x 1.40	242 x 175 x 35.5/ 9.53 x 6.89 x 1.40	430 x 201 x 42/ 16.93 x 7.91 x 1.65	431 x 292 x 43.5/ 16.97 x 11.50 x 1.71	430 x 487 x 89/ 16.93 x 19.17 x 3.50
Item weight (kg/lb.)	0.42/0.93	0.38/0.84	1.2/2.65	1.2/2.65	1.2/2.65	2.8/6.17	4.7/10.36	10.5/23.15
Packing dimensions (W x D x H)(mm/in.)	305 x 205 x 106/ 12.01 x 8.07 x 4.17	305 x 205 x 106/ 12.01 x 8.07 x 4.17	375 x 238 x 108/ 14.76 x 9.37 x 4.25	296 x 158 x 241/ 11.65 x 6.22 x 9.49	296 x 158 x 241/ 11.65 x 6.22 x 9.49	539 x 184 x 321/ 21.22 x 7.24 x 12.64	529 x 411 x 194/ 20.83 x 16.18 x 7.64	607 x 551 x 295/ 23.90 x 21.70 x 11.61
Packing weight (kg/lb.)	1.1/2.43	1/2.20	2.4/5.29	2.7/5.95	3/6.61	6/13.22	6.5/14.33	14.2/31.31
Environmental Specifications								
Operating temperature	0°C to 40°C/32°F to 104°F	0°C to 40°C/32°F to 104°F	0°C to 40°C/32°F to 104°F	0°C to 40°C/32°F to 104°F	0°C to 40°C/32°F to 104°F	0°C to 40°C/32°F to 104°F	0°C to 40°C/32°F to 104°F	0°C to 40°C/32°F to 104°F
Storage temperature	-30°C to 60°C/-22°F to 140°F	-30°C to 60°C/-22°F to 140°F	-30°C to 60°C/-22°F to 140°F	-30°C to 60°C/-22°F to 140°F	-30°C to 60°C/-22°F to 140°F	-30°C to 60°C/-22°F to 140°F	-30°C to 60°C/-22°F to 140°F	-30°C to 60°C/-22°F to 140°F
Operating humidity	5% to 90% (Non-condensing)	5% to 90% (Non-condensing)	5% to 90% (Non-condensing)	5% to 90% (Non-condensing)	5% to 90% (Non-condensing)	5% to 90% (Non-condensing)	5% to 90% (Non-condensing)	5% to 90% (Non-condensing)

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.
*6: With SEM-DUAL or SEM-VPN module
*7: With SEM-DUAL module

Features

Firewall
- ICSA-certified firewall
- Routing and transparent (bridge) mode
- Zone-based access control list
- Stateful packet inspection
- User-aware policy enforcement
- SIP/H.323 NAT traversal
- ALG supports custom ports

Virtual Private Network (VPN)
- ICSA-certified IPSec VPN
- Algorithm: AES/3DES/DES
- Authentication: SHA-1/MD5
- Key management: Manual key/IKE
- Perfect forward secrecy (DH groups) support 1, 2, 5
- IPSec NAT traversal
- Dead peer detection/relay detection
- PKI (X.509) certificate support
- Centralize VPN support
- Simple wizard support
- Auto reconnect VPN
- VPN HA (redundant remote VPN gateways)

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 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

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

Application Patrol (except USG20/20W)
- Application, IM/P2P, stream base media, VoIP granular access control
- Detail access control of IM (chat, file transfer, video)
- Application and IM/P2P bandwidth control
- User authentication support
- IM/P2P signature auto update
- Support more than 15 catalogs IM and P2P
- Real-Time statistical reports
- Maximum/guaranteed bandwidth

Anti-Spam
- Zone to zone protection
- Transparently intercept mail via SMTP/POP3 protocols
- Blacklist/whitelist support
- Support DNSBL checking
- Spam tag support
- Statistics report

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

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

Networking
- Routing mode/bridge mode/mixed mode
- Layer 2 port grouping
- Ethernet/PPPoE
- NAT/PAT
- 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 (except USG20/20W)
- Per host session limit
- Guaranteed bandwidth
- Maximum bandwidth
- Priority-bandwidth utilization

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

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

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

Accessories

Security Extension Module (USG 2000)

Model	SEM-DUAL	SEM-VPN
Product Photo		
Features	For customers requiring full security features of both VPN and UTM threat protections, the SEM-DUAL unleashes the full VPN and UTM performance of the ZyWALL USG 2000 platform. • SecuASIC CIP-3001 for UTM acceleration (Anti-Virus and IDP) • Advanced VPN Crypto to boost VPN performance	For customers requiring intensive VPN applications to build a mighty VPN concentrator in the central site and the highest level of redundancy, the specialized SEM-VPN application greatly accelerates VPN performance. • Advanced VPN Crypto to boost VPN performance
System Performance		
VPN Throughput (AES)^{*8} (Mbps)	600	600
UTM Throughput (AV+IDP)^{*9} (Mbps)	400	100
Max. IPSec VPN Tunnels	2,000	2,000
Max SSL VPN Users	750	750
Physical Specifications		
Dimensions (W x D x H)(mm/in.)	199.2 x 212 x 36.3/7.84 x 8.35 x 1.43	199.2 x 212 x 36.3/7.84 x 8.35 x 1.43
Weight (g/lb.)	410/0.91	410/0.91
Environmental Specifications		
Operating temperature	0°C to 40°C/32°F to 104°F	0°C to 40°C/32°F to 104°F
Storage temperature	-30°C to 60°C/-22°F to 140°F	-30°C to 60°C/-22°F to 140°F
Operating humidity	5% to 90% (Non-condensing)	5% to 90% (Non-condensing)

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	Connector	Wavelength	Max Transmission Distance	Optical Budget	Laser Transmitter Characteristics		Receiver Characteristics	
					Maximum Launch Power	Minimum Launch Power	Optical Receiver Sensibility	Maximum Input Power
SFP-SX-D	LC	850 nm	550 m	7.5 dB	-4 dBm	-9.5 dBm	-17 dBm	-3 dBm
SFP-LX-10-D	LC	1310 nm	10 km	10.5 dB	-3 dBm	-9.5 dBm	-20 dBm	-3 dBm
SFP-LHX1310-40-D	LC	1310 nm	40 km	21 dB	+3 dBm	-2 dBm	-23 dBm	-3 dBm
SFP-ZX-80-D	LC	1550 nm	80 km	24 dB	+5 dBm	0 dBm	-24 dBm	-3 dBm

Wireless Radio Information (USG 20W)

Model		USG 20W
Maximum Output Power		
802.11b	11 Mbps	18.5 dBm
802.11g	54 Mbps	15.5 dBm
802.11n	20 MHz	15.5 dBm
	40 MHz	12.5 dBm
Radio Sensitivity		
802.11b	11 Mbps	≤ -83 dBm
802.11g	54 Mbps	≤ -70 dBm
802.11n	20 MHz	≤ -64 dBm
	40 MHz	≤ -61 dBm