



Security on a New Level -The Future Is Ahead. Stay Ahead with ZyXEL USGs.

- Ultra-high performance and protection
- Comprehensive support to IPv6
- Supported various VPN solutions (IPSec/SSL/2TP)
 - Zero-configuration remote access with EASY VPN
 - Support L2TP VPN on mobile device (iPhone and Android phone)
- ICSA Firewall, IPSec certification
- Real-time, dynamic malware protection
- High Availability (HA)

Utilizing networks to access internal and external mission-critical applications are common, and important as well, for small and medium-sized businesses. As faster networks bring more convenience and efficiency, businesses are facing challenges from sophisticated attacks and even cybercrime that would cause interrupted communications, degraded performance and loss of valuable information; however traditional firewalls are not capable of protecting business from such network attacks.

The ZyXEL USG 300/1000/2000 Series are security platforms that offers ultra-high performance, deep packet inspection and all-in-one multi-threat protection not only to block the latest attack combinations including intrusion attempts, viruses, worms, phishing, spyware, spam and many other malware types effectively, but also to secure remote access among branch offices, partners and customers. The USG's real-time threat detection and continuous update services provide the fastest response speed in the networking industry to deter the evolving security threats before the business is affected. The ZyXEL USG 300/1000/2000 Series is ideal for small- and medium-size businesses to safeguard their network environments.

Benefits

Ultra-high performance and protection to secure business networks

The ZyXEL USG 300/1000/2000 Series delivers wire-speed performance and integrated threat management for wired networks. The USG Series provides firewall throughputs of from 350 Mbps to 2 Gbps that enables businesses to protect critical applications and networks without affecting availability or performance. In addition, the USG's unique built-in clean-traffic architecture can prevent risks such as viruses, worms, Trojan Horses, spyware, phishing attacks and other emerging Internet threats. In short, the architecture can assure clean and secure network environments for business users.



Comprehensive IPv6 support to ensure investment protection

The ZyXEL USG Series is IPv6-ready today and is certified with "IPv6 Ready" gold logo. With IPv6 feature enabled, the USG Series ensures businesses with a smooth migration path from the IPv4-based networks to the full IPv6 infrastructure. It assigns IPv6 addresses to clients and passes the IPv6 traffics through the IPv4 environment. The USG Series supports dual-stack and IPv4 tunneling (6rd and 6to4 transition tunnel) implementations for Internet connectivity to access IPv6 applications. The comprehensive IPv6 features built into the USG Series ensure not only future-ready connectivity but also investment protection for businesses. IPv6 applications.

USG 300/1000/2000
Unified Security Gateway



Various VPN solutions to simplify secure access

Establishing VPN tunnels is a good solution to provide a safe way to access necessary network resources remotely with any device anytime, anywhere. However due to the complicated configuration, it could be quite difficult for non-technical employees such as sales people to use. The ZyXEL USG Series is equipped with the "EASY VPN" solution to push configuration files to the VPN clients automatically; this eliminates the configuration efforts while securing the access at the same time. In addition, the USG Series supports L2TP VPN technology on iPhones, Android phones and many other mobile devices as L2TP VPN enables employees in remote places to connect to the headquarters with easy and free access.

Real-time, dynamic malware protection to safeguard business networks

Web security powered by BlueCoat and Commtouch

With more valuable information being placed on the data cloud, impacts from the ever-growing cybercrime should be treated seriously. As modern malware become very sophisticated and difficult to repel, the USG's content filter from Blue Coat and Commtouch, the leading solution provider, reduces costs and extends protection by integrating a comprehensive, continuously updated database featuring millions of URLs, IP addresses and domains. With the content filter, the USG Series not only enables real-time protection to deter emerging Web threats including malware, phishing and Zombies/bots, but also monitors or blocks certain sites to maintain employee productivity.

Email security powered by Commtouch

The ZyXEL USG Series delivers industry-leading protection, powered by Commtouch, against spam, phishing and virus-laden emails. The extremely high performance of Commtouch technology comes from the unique recurrent pattern detection (RPD) mechanism that possesses its superior capability through analyzing millions of new patterns each day (24x7x365) to block all the associated messages real-time. In addition, the USG applies sender-based IP reputation to remove over 80% of unwanted mails and to take advantage of the zero-hour virus outbreak protection feature, which is capable of blocking or delaying suspicious messages hours before commercial anti-virus signatures are available.

High Availability (HA) ensures non-stop business operations

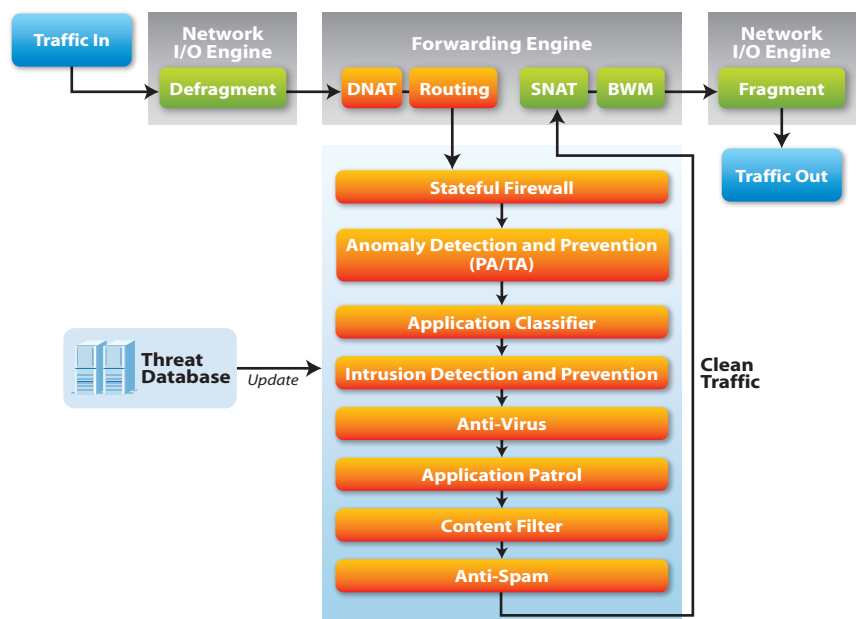
Loss of mission-critical connection can cause serious, and sometimes disastrous, consequences to businesses. The ZyXEL USG 300/1000/2000 Series provides HA features to guarantee a secure, reliable connection between the protected network and the Internet.

- Multiple WAN ports and configurable load balancing between ports.
- An auxiliary (backup) Internet connection known as out-of-band management.
- A backup USG in case the master USG fails (Device HA).

Key Applications

Unique clean-traffic architecture

The ZyXEL USG's clean-traffic architecture protects against network risks like 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.



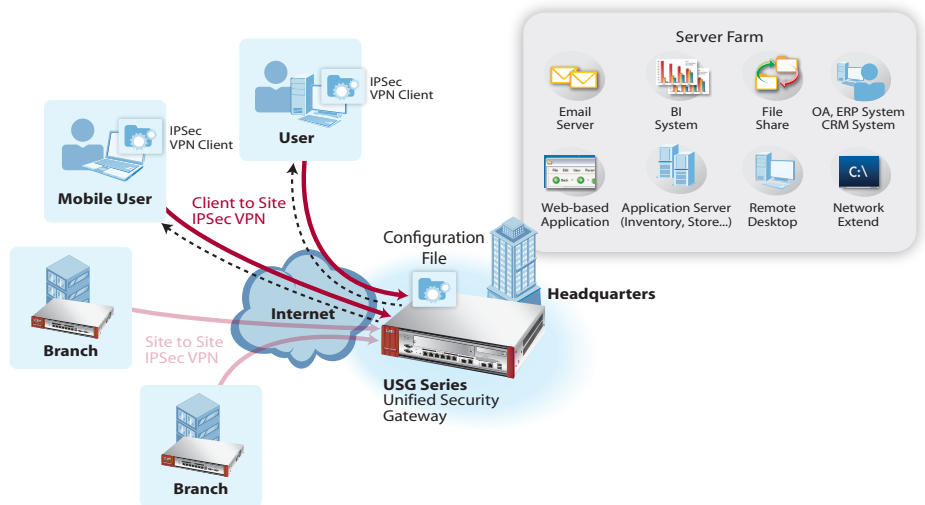
EASY VPN — zero configuration remote access

When establishing VPN tunnels, it could be quite difficult for non-technical employees to use due to the complicated configuration.

The ZyXEL USG Series is equipped with the "EASY VPN" solution to push configuration files to the VPN clients automatically; this eliminates the configuration efforts while securing the access at the same time.

Easy provisioning for IPSec VPN client

- USG automatically provides configuration file to the client.



Content Filter stops malware and Web threats

The ZyXEL 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.



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 ZyXEL USG Series prevents the Internet connection from being abused to minimize bandwidth waste or human resource policy violations. The USG Series provides granular control over the usage of social networking applications.

Without social network control






Low Productivity

With social network control



High Productivity

Specifications

Model	USG 300	USG 1000	USG 2000	
Product photo				
Hardware Specifications				
10/100/1000 interfaces (Copper)	7	5	6	
Dual personality GbE (SFP/RJ45)	-	-	2	
USB ports	2	2	2	
SEM Slot (Security extension module)	-	-	1	
Card slot	2	1	1	
System Capacity & Performance ^{*1}				
SPI firewall throughput ^{*2} (Mbps)	350	400	2,000	
VPN throughput (AES) ^{*3} (Mbps)	130	180	600 ^{*6}	
UTM throughput (AV+IDP) ^{*4} (Mbps)	80	100	400 ^{*7}	
Unlimited user licenses	Yes	Yes	Yes	
Max. sessions ^{*5}	60,000	500,000	1,000,000	
New session rate	1,500	12,000	20,000	
Max. concurrent IPSec VPN tunnels	200	1,000	2,000	
Max. concurrent SSL VPN users	25	250	750 ^{*7}	
Included SSL VPN users	2	5	5	
Customizable zone	Yes	Yes	Yes	
IPv6 support	Yes	Yes	Yes	
Power Requirement				
Input voltage	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	35 W Max.	80 W Max.	200 W Max.	
Power consumption (watt)	35	80	200	
Physical Specifications				
Item	Dimensions (WxDxH)(mm/in.)	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
	Weight (kg/lb.)	2.8/6.17	4.7/10.36	10.5/23.15
Packing	Dimensions (WxDxH)(mm/in.)	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 11.6
	Weight (kg/lb.)	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			
Storage temperature	-30°C to 60°C/-22°F to 140°F			
Operating humidity	5% to 90% (non-condensing)			
MTBF (hr)	180,382	51,611	99,141	

Note:

*1: Actual performance may vary depending on network conditions and activated applications.

*2: Maximum throughput based on RFC 2544 (1,518-byte UDP packets).

*3: VPN throughput measured based on RFC 2544 (1,424-byte UDP packets).

*4: UTM (AV and IDP) throughput measured using the industry standard IXIA IxLoad testing tool (1,460-byte HTTP packets).

*5: Maximum sessions measured using the industry standard IXIA IxLoad testing 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

IPv6 Support

- IPv6 Ready gold logo certified
- Dual stack
- IPv4 tunneling (6rd and 6to4 transition tunnel)
- Host/Router/Firewall

Virtual Private Network (VPN)

- ICSA-certified IPSec VPN
- Algorithm: AES/3DES/DES
- Authentication: SHA-1, SHA-2/MD5
- Key management: Manual key/IKE
- Perfect forward secrecy (DH groups) support 1, 2, 5
- IPSec NAT traversal
- Dead peer detection/relay detection

Features

Virtual Private Network (VPN)

- 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)*¹

- 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

Application Intelligence*¹ (Application Patrol)

- Identify more than 600 applications, including IM, P2P, social network, stream media, VoIP, and others
- Support application granularity control
- Manage use of Skype/MSN, GoogleTalk, Facebook at business hours, or never
- Block all use of P2P and Games applications all the time (or during business hours)
- Bandwidth management for P2P, Stream Media, File Transfer, or particular applications
- Daily check and auto update application signatures
- Real-Time statistical reports

Anti-Virus*²

- 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

Anti-Spam

- Zone to zone protection
- Transparently intercept mail via SMTP/POP3 protocols
- POP3/SMTP port configurable
- Sender-based IP Reputation Filter
- Commtouch RPD Query
- Zero-hour Virus Outbreak Protection
- X-Header Support
- Blacklist/whitelist support
- Support DNSBL checking
- Spam tag support
- Statistics report

High Availability

- Active-Passive mode
- Device failure detection and notification
- Support ICMP and TCP ping check
- Link monitoring
- Auto-Sync configurations

Content Filtering (BlueCoat and Commtouch)*³

- 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 and Commtouch)
- 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
- 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

Certification

- Safety
 - CSA International
- Emission (EMC)
 - FCC Part15 (Class A)
 - CE EMC (Class A)

Note:

*1: Available for USG 300/1000/2000 models with Intrusion Detection/Prevention(IDP) subscription.



*2: Available for USG 300/1000/2000 models with Anti-Virus subscription.

*3: Available for all USG models with Content Filtering subscription.



Accessories

Security Extension Module (USG 2000)

Model	SEM-DUAL	SEM-VPN
Product photo		
Features	<p>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 USG 2000 platform.</p> <ul style="list-style-type: none"> • SecuASIC CIP-3001 for UTM acceleration (Anti-Virus and IDP) • Advanced VPN Crypto to boost VPN performance 	<p>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.</p> <ul style="list-style-type: none"> • Advanced VPN Crypto to boost VPN performance
System Performance		
VPN throughput (AES)*¹ (Mbps)	600	600
UTM throughput (AV+IDP)*² (Mbps)	400	100
Max. IPSec VPN tunnels	2,000	2,000
Max SSL VPN users	750	750
Physical Specifications		
Dimensions (WxDxH)(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:

*1: VPN (AES) HTTP protocol with 1,460 bytes packet size. Testing done with multiple flows.

*2: UTM (AV+IDP) throughput measured using industry standard Ixia IxLoad test tool against.

Transceivers

Model Name	Connector	Wavelength	Max Transmission Distance (km/yd)	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	0.55/601	7.5 dB	-4 dBm	-9.5 dBm	-17 dBm	-3 dBm
SFP-LX-10-D	LC	1310 nm	10/10936	10.5 dB	-3 dBm	-9.5 dBm	-20 dBm	-3 dBm
SFP-LHX1310-40-D	LC	1310 nm	40/43744	21 dB	+3 dBm	-2 dBm	-23 dBm	-3 dBm
SFP-ZX-80-D	LC	1310 nm	80/87488	24 dB	+5 dBm	0 dBm	-24 dBm	-3 dBm

3G Card Support

Please visit http://www.zyxel.com/products_services/smb_security_appliances_and_services.shtml and find the following path:
ZyXEL 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



Copyright © 2013 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.

