ZyXEL

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

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	All ZyWALL Models support, 10 nodes 25 nodes 50 nodes 100 nodes 300 nodes 1000 nodes	All ZyWALL Models support, 1 device 5 devices 25 devices 100 devices
	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*	Yes	Yes	Yes		
	2 years	Yes*	Yes	Yes	Yes		
USG 20	1 year	-	-	-	Yes		
	2 years	-	-	-	Yes		
USG 20W	1 year	-	-	-	Yes		
	2 years	-	-	-	Yes		

*: Available in Q1 2011

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 5 to 50 SSL Tunnels 5 to 250 SSL Tunnels 25 to 50 SSL Tunnels 25 to 250 SSL Tunnels 50 to 250 SSL Tunnels	For Client PC's Software client 1 license Software client 5 licenses Software client 10 licenses Software client 50 licenses
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

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.

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

usg-series-001   09/10

ZyXEL

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 (ZSDN)**

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, 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.

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 mails (spam). Without intelligent detection and proactive blocking, users have to go through the tedious and time-consuming task of sieving 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 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 Vantage CNM (Centralized Network Management), users can achieve the follow 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 expanse.

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

ZyXEL

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

ZyXEL

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.
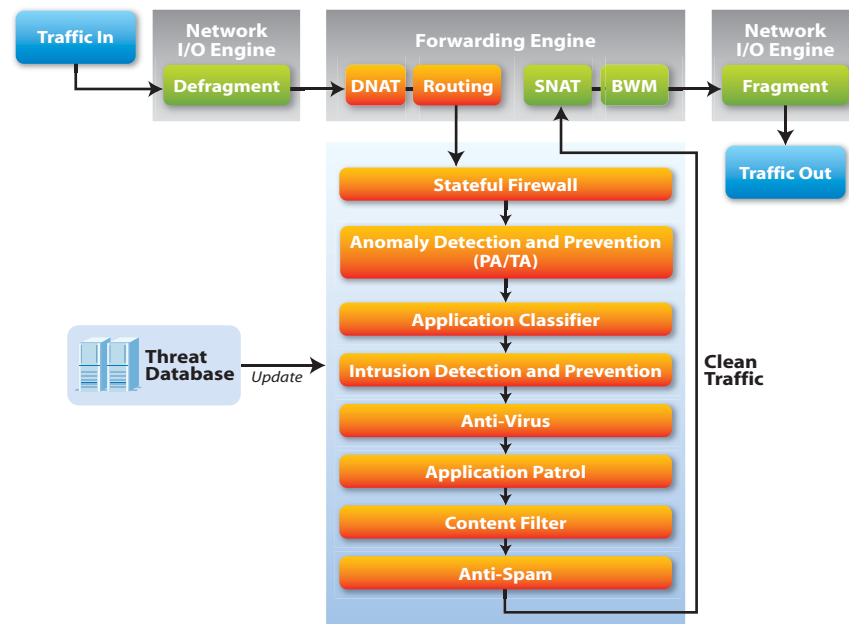

Endpoint security

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™ AV 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.
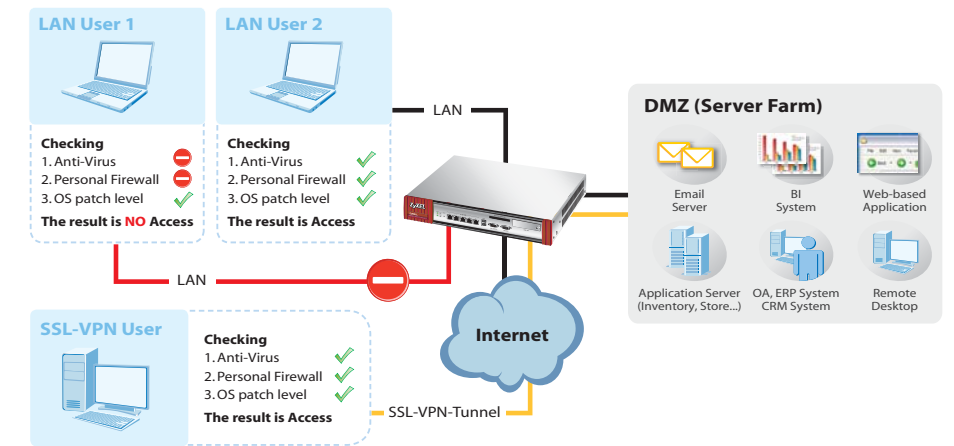
The USG's new «End Point Security» (EPS) feature helps to ensure that all clients meet the corporate security policies, i.e. It checks if AV software is installed.

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.
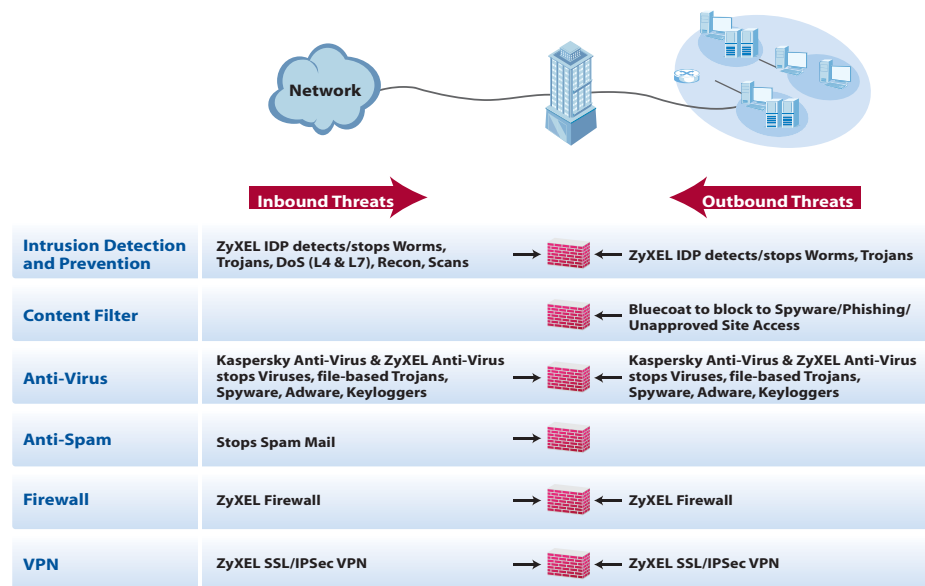
High performance

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.
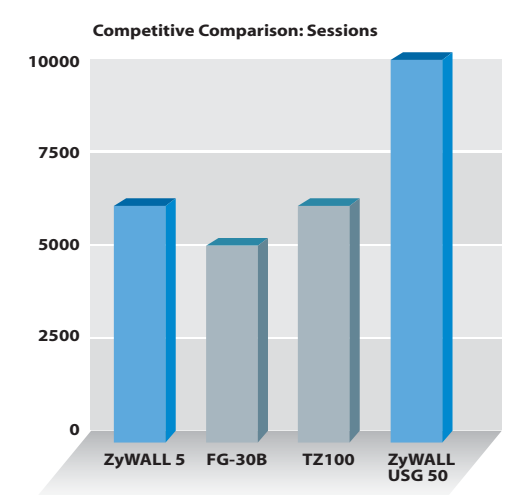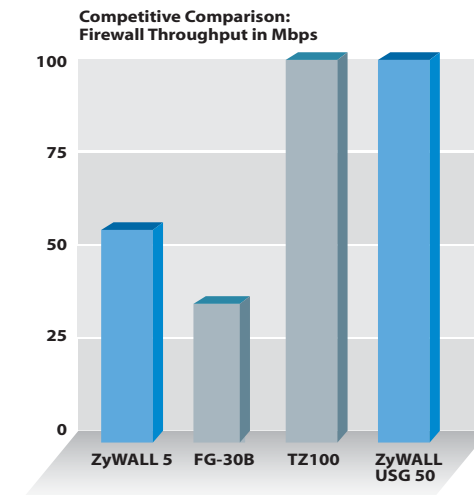
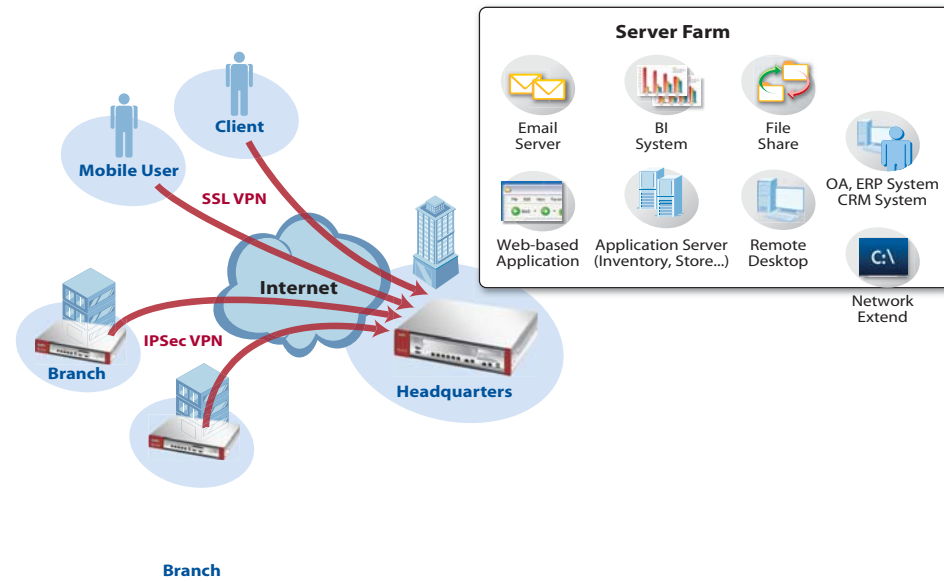Source : Performance numbers are from ZyXEL, SonicWALL, Fortinet website

ZyXEL

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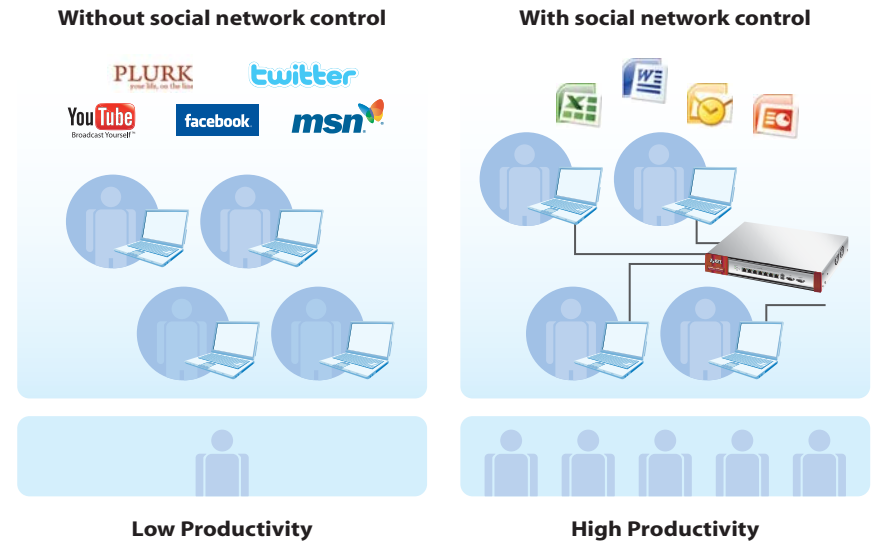### (20/50/100/200/300/1000/2000 Series)

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.

Client
Mobile User
SSL VPN
Branch
Internet
IPSec VPN
Branch
Headquarters

Server Farm

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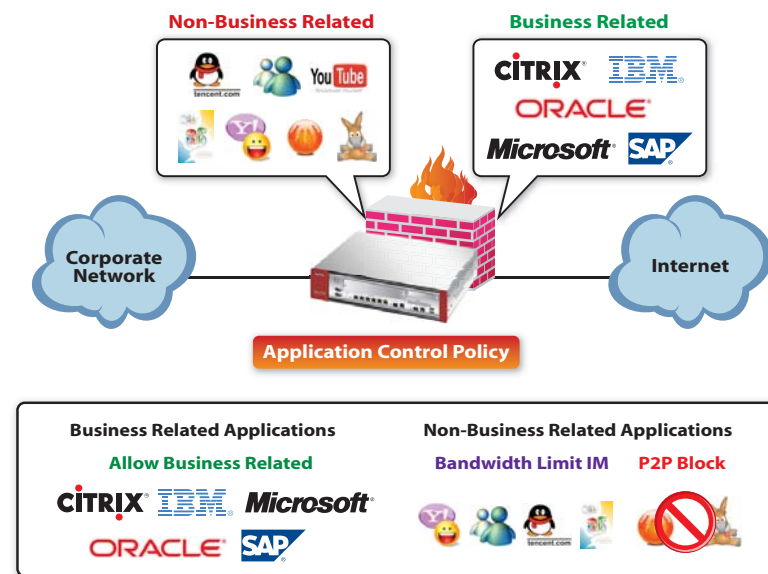OA, ERP System CRM System
Network Extend

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.

Without social network control

PLURK
twitter
YouTube
facebook
msn

With social network control

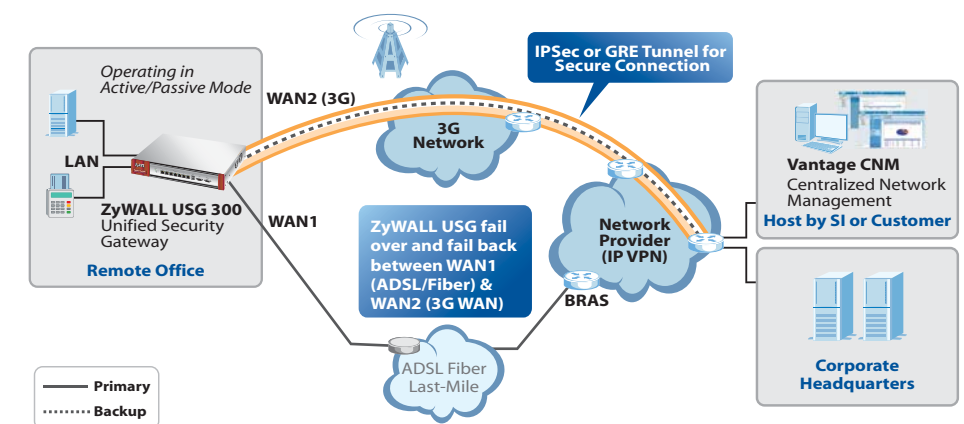**Low Productivity**   **High Productivity**

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
tencent.com
YouTube

Business Related
CITRIX
IBM
ORACLE
Microsoft
SAP

Corporate Network
Internet

Application Control Policy

Business Related Applications
Allow Business Related
CITRIX IBM Microsoft
ORACLE SAP

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

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.

Operating in Active/Passive Mode
WAN2 (3G)
LAN
ZyWALL USG 300 Unified Security Gateway
WAN1
Remote Office
3G Network
IPSec or GRE Tunnel for Secure Connection
ZyWALL USG fail over and fail back between WAN1 (ADSL/Fiber) & WAN2 (3G WAN)
ADSL Fiber Last-Mile
BRAS
Network Provider (IP VPN)
Vantage CNM Centralized Network Management
Host by SI or Customer
Corporate Headquarters

— Primary
····· Backup

ZyXEL

ZyXEL

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 desirably 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.

Device HA: Master Fails and Backup Takes Over
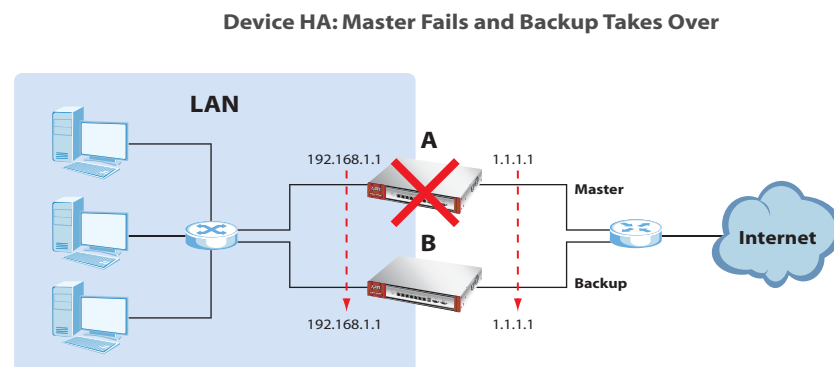
Anti-Spam service

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.
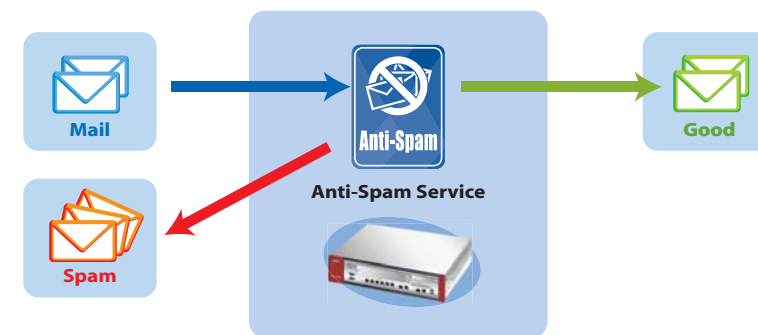
Comprehensive reporting system

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**

ZyWALL USG Series provides built-in reporting system to collect data and view various statistics about traffic passing through your ZyWALL.

● **Vantage Report Centralize Reporting System**

Vantage Report is a cost-effective solution that allows administrators to easily monitor and analyze report of ZyWALL Internet Security Appliances from any location. It delivers rich formats of statistical report for IT staff with thorough understanding about bandwidth usage, security event and web traffic analysis.
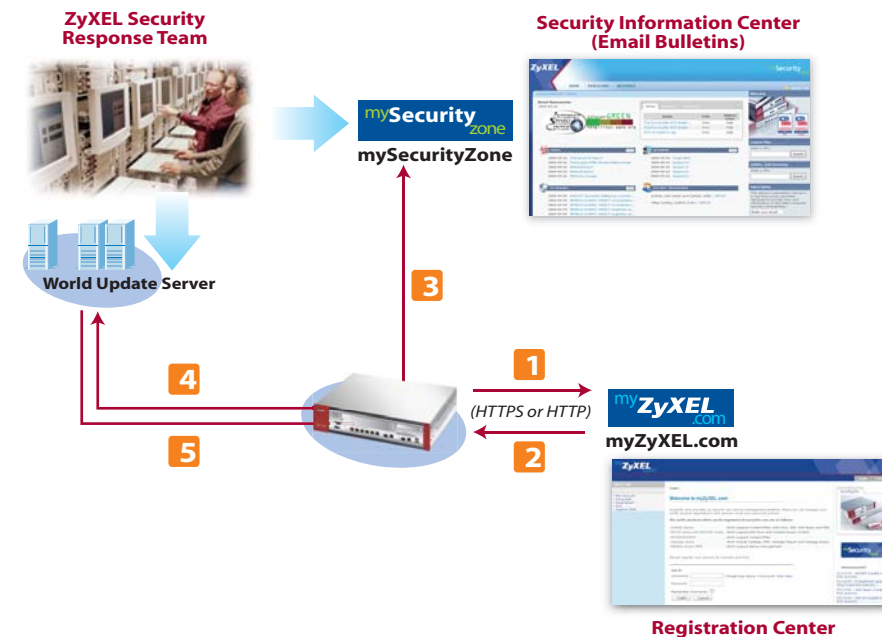
Monitor

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 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.

ZyXEL

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

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/H.323 NAT traversal
- ALG supports custom ports

Virtual Private Network (VPN)
- ICSA-certified IPSec VPN
- PPTP, L2TP, IPSec
- 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
- 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—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 BlueCoat)
- Unlimited user licenses support
- Customize warning messages and redirect URL

Networking
- Routing mode/bridge mode/mixed mode
- Layer 2 port grouping
- Ethernet/PPPoE
- 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)
- Out-of-band management (AUX)
- 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

ZyXEL

Security Extension Module (USG 2000 only)

Model	SEM-DUAL	SEM-VPN
Product Photo		
Features	For customers require full security features both VPN and UTM threat protections. The SEM-DUAL unleashes full horse power of the ZyWALL USG 2000 platform with mighty VPN and UTM performance. • SecuASIC CIP-3001 for UTM Acceleration (Anti-Virus and IDP) • Advanced VPN Crypto to Boost up VPN Performance	For customers in need of intensive VPN applications to build up mighty VPN concentrator in central site while requires highest level of redundancy. Specialized in VPN applications, the SEM-VPN accelerates VPN performance. • Advanced VPN Crypto to Boost up VPN Performance
System Performance		
VPN Throughput (AES)[*7]	400 Mbps	400 Mbps
UTM Throughput (AV+IDP)[*8]	400 Mbps	100 Mbps
Max. IPSec VPN Tunnels	2,000	2,000
Max SSL VPN Users	750	750
Environmental Specifications		
Operating Temperature	0C to 40C	0C to 40C
Storage Temperature	-30C to 60C	-30C to 60C
Operating Humidity	5% to 90% (non-condensing)	5% to 90% (non-condensing)
Physical Specifications		
Dimensions, (W) x (D) x (H) mm	199.2 x 212 x 36.3	199.2 x 212 x 36.3
Weight, g	410	410

Note:
*7: VPN (AES) HTTP protocol with 1,460 bytes packet size. Testing done with multiple flows.
*8: 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

ZyXEL

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

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	• 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	• 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	100	100	100	150	200	300	400	2,000
VPN Throughput (3DES)[*2], Mbps	30	30	50	60	75	100	150	400[*4]
UTM Throughput (AV+IDP)[*3], Mbps	-	-	15	30	40	60	80	400[*5]
WiFi Throughput, Mbps	60	-	-	-	-	-	-	-
Unlimited User Licenses	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Max. Sessions[*6]	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	2	2	5	50	100	200	1,000	2,000
Max. Concurrent SSL VPN Users	1	1	5	5	10	25	250	750[*1*2]
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
Environmental Specifications								
Operating Temperature	0C to 40C	0C to 40C	0C to 40C	0C to 40C	0C to 40C	0C to 40C	0C to 40C	0C to 40C
Storage Temperature	0C to 40C	0C to 40C	0C to 40C	-30C to 60C	-30C to 60C	-30C to 60C	-30C to 60C	-30C to 60C
Operating Humidity	20% to 95% (non-condensing)	20% to 95% (non-condensing)	20% to 95% (non-condensing)	5% to 90% (non-condensing)	5% to 90% (non-condensing)	20% to 90% (non-condensing)	5% to 90% (non-condensing)	5% to 90% (non-condensing)
Physical Specifications								
Dimensions, (W) x (D) x (H) mm	216 x 140 x 33	216 x 140 x 33	242 x 167 x 35.5	242 x 175 x 35.5	242 x 175 x 35.5	430 x 201 x 42	431 x 292 x 43.5	430 x 487 x 89
Weight, kg	0.42	0.38	1.2	1.2	1.2	2.8	4.7	10.5

Note:
*1: Testing Methodologies: Maximum performance based on RFC 2544 (UDP packets, 1,518 bytes). Actual performance may vary depending on network conditions and activated services.
*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: With SEM-DUAL/SEM-VPN module
*5: With SEM-DUAL module
*6: Max sessions measured using industry standard Ixia IxLoad test tool.