



New Era for SMB Security Network Protection

- High performance with 8-in-1 Security
- Exclusive ZyXEL SecuASIC™ accelerating technology
- Protection from Spyware, Phishing, Viruses, and Spam
- IM (Instant messaging), P2P (Peer-to-peer) Applications, and Granular Control



Integrated Internet
Security Appliance with
Unified Threat
Management

ZYWALL
5/35/70
UTM SERIES

Benefits

UTM is an Emerging Trend in Network Security

Gone are the days when a dedicated firewall is sufficient to fend off hackers from cooperate networks. Unified Threat Management (UTM) is an emerging trend in the network security appliance market. Always on the cutting edge, ZyXEL's ZyWALL 5/35/70 UTM series is capable of outperforming the current ZyWALL 5/35/70 series by up to 20 times with just a ZyWALL Turbo Card. This new technology introduces a new all-in-one network security device that provides content filtering, anti-virus, anti-spam and intrusion detection services traditionally handled by multiple systems.

High-performance All-in-one Design

From a business perspective, IT managers should consider an "enterprise approach" for comprehensive security. They can now utilize all-in-one appliances, such as ZyXEL's 8-in-1 UTM solution, for solid protection and performance. All of the following features are now offered in one box and controlled through a single unified interface: Anti-Virus, IDP, Anti-Spam, Firewall, VPN, Load Balancing, Bandwidth Management and Content Filtering.

Empowering ZyWALL Performance with Turbo Card

Take advantage of secure protection from virus attacks, hackers, and spam. Imagine, no more worrying about spyware, adware, or other potential threats to your computer and valuable data. Make the Internet safe for your PCs and Network.

Upgradeable Design with ZyWALL Turbo Card within 6-Step

In an increasingly complex network environment the integrated ZyWALL UTM provides streamlined management efforts, easy installation, and multiple layers of network protection.

Specifications

System Specifications

Firewall (ICSA Certified)

- IP Protocol/Packet Filter
- DoS and DDoS Protections
- Stateful Packet Inspection
- Real time E-mail alerts
- Reports and Logs
- Transparent Firewall

VPN (ICSA Certified)

- Manual key, IKE
- PKI (X.509)
- Encryption (DES, 3DES and AES)
- Authentication (SHA-1 and MD5)
- IPSec NAT Traversal
- Xauth User Authentication (Internal Database and External RADIUS)
- DH1/2, RSA signature

Anti-Virus/IDP

(Intrusion Detection and Prevention)

- Enabled and Activated by a ZyWALL Turbo Card (ZyXEL SecuASIC inside)
- Virus, Worm, trojan, backdoor, buffer overflow and port scan protection
- P2P, IM, web attack, protection
- Automatic/scheduling signatures update
- Real-time attack alerts and logs

Anti-Spam

- Spam, Phishing prevention
- Configurable white and black lists
- SMTP, POP3 support
- External Spam database

Content Filtering

- Web page blocking by URL keyword
- IKE + PKI support
- External database content filtering
- Java/ActiveX /Cookie/News blocking

Traffic Management

- Guaranteed/Maximum Bandwidth
- Policy-based Traffic shaping
- Priority-bandwidth utilization
- Load Balancing (ZyWALL 35/70/35 UTM/70 UTM available)
- Bandwidth Management
- Static Routes

High Availability (ZyWALL 35/70/35 UTM/70 UTM available)

- Auto fail-over, fail-back
- Dial Backup
- Dual WAN ports for WAN backup and Load Balancing

System Management

- Embedded Web Configurator (HTTP and HTTPS)
- Menu-driven SMT (System Management Terminal) management
- CLI (Command Line Interpreter)
- Remote Management via Telnet or Web
- SNMP manageable
- Firmware Upgrade (web configurator, TFTP/FTP/SFTP)
- ZyXEL Centralized Network Management (Vantage CNM) support

Logging/Monitoring

- Centralized Logs
- Attack alert
- System status monitoring
- Syslog

Protocol Support

- PPP (Point-to-Point Protocol) link layer protocol
- Transparent bridging for unsupported network layer protocols
- DHCP Server/Client/Relay
- RIP I/RIP II
- ICMP
- SNMP v1 and v2c with MIB II support (RFC 1213)
- IP Multicasting IGMP v1 and v2
- IGMP Proxy
- UPnP

Hardware Specifications

Power Specification

- ZyWALL 70/70 UTM: 100 ~ 240 VAC
- ZyWALL 5/35/5 UTM/35 UTM: 12V DC

Fuse Specification

- ZyWALL 70/70 UTM: T 0.5 Amp, 250 VAC

Physical Specification

- Reset Button: Restores factory default settings
- Console: RS-232 DB9F
- Dial Backup: RS-232 DB9M
- Extension Card Slot: For installing an optional ZyXEL wireless LAN card or a ZyWALL Turbo Card

Ethernet Interface

ZyWALL 5/5 UTM

- LAN/DMZ: 4 ports auto MDI/MDI-X 10/100 Mbps Ethernet
- WAN: 1 port auto MDI/MDI-X 10/100 Mbps Ethernet

ZyWALL 35/35 UTM

- LAN/DMZ: 4 ports auto MDI/MDI-X 10/100 Mbps Ethernet
- WAN: 2 ports auto MDI/MDI-X 10/100 Mbps Ethernet

ZyWALL 70/70 UTM

- LAN: 1 port auto MDI/MDI-X 10/100 Mbps Ethernet
- DMZ: 4 ports auto MDI/MDI-X 10/100 Mbps Ethernet
- WAN: 2 ports auto MDI/MDI-X 10/100 Mbps Ethernet

Dimensions

- ZyWALL 5/5 UTM 242(W) x 175(D) x 35.5(H) mm
- ZyWALL 35/35 UTM 242(W) x 175(D) x 35.5(H) mm
- ZyWALL 70/70 UTM 355(W) x 200(D) x 55(H) mm

Weight

- ZyWALL 5/5 UTM: 1,200g
- ZyWALL 35/35 UTM: 1,200g
- ZyWALL 70/70 UTM: 2,600g

Environmental Specification

- Operation Temperature: 0°C ~ 50°C
- Storage Temperature -30°C ~ 60°C
- Operation Humidity: 20% ~ 95% RH (non-condensing)
- Storage Humidity: 20% ~ 95% RH (non-condensing)

Certification

- EMC: FCC Class B, CE-EMC Class B, C-Tick Class B, VCCI Class B
- Safety: CSA International, CE EN60950-1

Feature Matrix

Model name	ZyWALL P1	ZyWALL 2	ZyWALL 5	ZyWALL 35	ZyWALL 70	ZyWALL 5 UTM	ZyWALL 35 UTM	ZyWALL 70 UTM
Performance								
Firewall Throughput	80Mbps	12Mbps	65Mbps	70Mbps	90Mbps	65Mbps	70Mbps	90Mbps
VPN 3DES/AES Throughput	30Mbps	2.2Mbps	25Mbps	30Mbps	40Mbps	25Mbps	30Mbps	40Mbps
User Licenses								
Concurrent Sessions	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Simultaneous IPSec VPN connections	2,048	1,048	4,000	10,000	10,000	4,000	10,000	10,000
Physical Specification								
Ports (10/100Mbps Auto sensing & MDI/MDIX)	1xLAN, 1xWAN	4xLAN, 1xWAN	4xLAN/DMZ, 1xWAN	4xLAN/DMZ, 2xWAN	1xLAN, 4xDMZ, 2xWAN	4xLAN/DMZ, 1xWAN	4xLAN/DMZ, 2xWAN	1xLAN, 4xDMZ, 2xWAN
Extension Card Slot	n/a	n/a	Wireless Card ZyWALL Turbo Card (UTM Upgrade)	Wireless Card ZyWALL Turbo Card (UTM Upgrade)	Wireless Card ZyWALL Turbo Card (UTM Upgrade)	ZyWALL Turbo Card	ZyWALL Turbo Card	ZyWALL Turbo Card
RS-232 console	n/a	x	x	x	x	x	x	x
Power Supply	5VDC	12VDC	12VDC	12VDC	100 ~ 240VDC	12VDC	12VDC	100 ~ 240VDC
Rack-Mounted	n/a	n/a	x	x	x	x	x	x
Wall-Mounted	n/a	x	x	x	n/a	x	x	n/a
Dimensions (W x D x H, mm)	129 x 82 x 20	181 x 128 x 36	242 x 175 x 35.5	242 x 175 x 35.5	355 x 200 x 55	242 x 175 x 35.5	242 x 175 x 35.5	355 x 200 x 55
Weight	130g	330g	1,200g	1,200g	2,600g	1,200g	1,200g	2,600g
Mode of Operation								
Routing/NAT/SUA Mode	x	x	x	x	x	x	x	x
Transparent Mode	x*	n/a	x	x	x	x	x	x
Dial Backup	n/a	x	x	x	x	x	x	x
Firewall (ICSA Certified)								
IP Protocol/Packet Filter	x	x	x	x	x	x	x	x
DoS and DDoS protections	x	x	x	x	x	x	x	x
Stateful Packet Inspection	x	x	x	x	x	x	x	x
Transparent Firewall	x*	n/a	x	x	x	x	x	x
Web Content Filtering	n/a	x	x	x	x	x	x	x
VPN (ICSA Certified)								
Manual key, IKE	x	x	x	x	x	x	x	x
PKI (X.509)	x	x	x	x	x	x	x	x
Encryption (DES, 3DES and AES)	x	x	x	x	x	x	x	x
Authentication (SHA-1 and MD5)	x	x	x	x	x	x	x	x
IPSec NAT Traversal	x	x	x	x	x	x	x	x
Xauth User Authentication (Internal Database and External RADIUS)	x	x	x	x	x	x	x	x
Content Filtering								
Internal Content Filtering (Java, Cookies, Active X blocking)	n/a	x	x	x	x	x	x	x
Internal Content Filtering (URL/Keyword blocking)	n/a	x	x	x	x	x	x	x
External Database Content Filtering	n/a	x (Bluecoat)	x (Bluecoat)	x (Bluecoat)	x (Bluecoat)	x (Bluecoat)	x (Bluecoat)	x (Bluecoat)
Anti-Virus/IDP								
Virus, worm, trojan, backdoor, buffer overflow, port scan protections	x*	n/a	UTM Upgradeable	UTM Upgradeable	UTM Upgradeable	x	x	x
P2P, IM, web attack protections	x*	n/a	UTM Upgradeable	UTM Upgradeable	UTM Upgradeable	x	x	x
Automatic/Scheduling signature update	x*	n/a	UTM Upgradeable	UTM Upgradeable	UTM Upgradeable	x	x	x
Real-time attack Alerts and Logs	x*	n/a	UTM Upgradeable	UTM Upgradeable	UTM Upgradeable	x	x	x
Anti-SPAM								
SPAM, Phishing prevention	x*	n/a	x	x	x	x	x	x
Configurable White/Black list	x*	n/a	x	x	x	x	x	x
SMTP, POP3 support	x*	n/a	x	x	x	x	x	x
Traffic Management								
Guaranteed/Maximum Bandwidth	n/a	n/a	x	x	x	x	x	x
Policy-based Traffic shaping	n/a	n/a	x	x	x	x	x	x
Priority-bandwidth utilization	n/a	n/a	x	x	x	x	x	x
High Availability (HA)								
Auto fail-over, fail-back	n/a	x	x	x	x	x	x	x
Dial Backup	n/a	x	x	x	x	x	x	x
Dual WAN ports for WAN backup and Load Balance	n/a	n/a	n/a	x	x	n/a	x	x
System Management								
WebGUI (HTTP and HTTPS)	x	x	x	x	x	x	x	x
Firmware Upgrade (WebGUI, TFTP/FTP/SFTP)	x	x	x	x	x	x	x	x
Vantage CNM	x	x	x	x	x	x	x	x
Wireless								
IEEE 802.11b Compliant	n/a	n/a	x	x	x	n/a	n/a	n/a
IEEE 802.11g Compliant	n/a	n/a	x	x	x	n/a	n/a	n/a
IEEE 802.1x Authentication (Internal Database and External RADIUS)	n/a	n/a	x	x	x	n/a	n/a	n/a
Logging/Monitoring								
Centralized Logs	x	x	x	x	x	x	x	x
Attack alert	x	x	x	x	x	x	x	x
System status monitoring	x	x	x	x	x	x	x	x

*Firmware upgradeable for future enhancement

ZyXEL's Solution to Top 4 Security Headaches

As network threats emerge with greater complexity, traditional passive methods of network defense has become obsolete. What you need is intelligent network security solutions that respond to threats and take proactive actions.

The following describes the four security problems on IT managers' top-unwanted list.

Virus Attacks

Malicious virus and worm attacks could cripple corporate networks and halt business transactions. In addition to severe financial impact, you also risk the lost of confidential, important information.

File Sharing and Messaging Application Abuse

With numerous file-sharing 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 file containing malicious viruses, but may also violate copyright issues and create legal hassles. Although the convenience of IM applications reduces communication cost between business partners, it could hamper business productivity when its use is non-work related.



Unsolicited Spams

As mass-mailing software and companies mushroomed on the Internet, your network is bombarded with massive amount of junk mails (aka. spam). Without intelligent detection and proactive blocking, users have to go through the tedious and time-consuming task of sieving through the overflowing mailbox. Worse yet, these unwanted mails usually contain inappropriate, luring or even criminal messages that would mislead your employees. Simply put, spam mails mean serious productivity loss.

Rampant Non-Work Related Surfing, Spyware, Phishing

Every employee uses the Internet for personal reasons at one point or another during work hours. Be they browsing through news headlines or visiting websites with questionable contents, they are exposing their computers to threats of invisible spyware or phishing. These hard-to-detect, self-embed software gather personal data or steal confidential business information all without the knowledge of the users.

Powered by Kaspersky, BlueCoat, Mailshell, ZyNOS4, ICSA Firewall, ICSA VPN



Content Control
from **BlueCoat**



mailshell™

ZyNOS4



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

Corporate Headquarters
ZyXEL Communications Corp.
Tel: +886-3-578-3942
Fax: +886-3-578-2439
Email: sales@zyxel.com.tw
<http://www.zyxel.com>
<http://www.zyxel.com.tw>

ZyXEL Denmark A/S
Tel: +45 39 55 07 00
Fax: +45 39 55 07 07
Email: sales@zyxel.dk
<http://www.zyxel.dk>

ZyXEL France SARL
Tel: +33 (0)4 72 52 97 97
Fax: +33 (0)4 72 52 19 20
Email: info@zyxel.fr
<http://www.zyxel.fr>

ZyXEL Hungary
Tel: +36-1-336-1646
Fax: +36-1-325-9100
Email: info@zyxel.hu
<http://www.zyxel.hu>

ZyXEL North America
Tel: +1-714-632-0882
Fax: +1-714-632-0858
Email: sales@zyxel.com
<http://www.us.zyxel.com>

ZyXEL Russia
Tel: +7 (095) 542-8920
Fax: +7 (095) 542-8925
Email: info@zyxel.ru
<http://www.zyxel.ru>

ZyXEL Sweden A/S
Tel: +46 (0) 31 744 77 00
Fax: +46 (0) 31 744 77 01
Email: sales@zyxel.se
<http://www.zyxel.se>

ZyXEL Ukraine
Tel: +380 44 494 49 31
Fax: +380 44 494 49 32
Email: sales@ua.zyxel.com
<http://www.ua.zyxel.com>

ZyXEL Czech s.r.o.
Tel: +420 241 091 350
Fax: +420 241 091 359
Email: info@zyxel.cz
<http://www.zyxel.cz>

ZyXEL Finland Oy
Tel: +358-9-4780 8400
Fax: +358-9-4780 8448
Email: sales@zyxel.fi
<http://www.zyxel.fi>

ZyXEL Germany GmbH.
Tel: +49 (0) 2405-6909 0
Fax: +49 (0) 2405-6909 99
Email: sales@zyxel.de
<http://www.zyxel.de>

ZyXEL Kazakhstan
Tel: +7-327-2-590-699
Fax: +7-327-2-590-689
Email: sales@zyxel.kz
<http://www.zyxel.kz>

ZyXEL Norway A/S
Tel: +47 22 80 61 80
Fax: +47 22 80 61 81
Email: sales@zyxel.no
<http://www.zyxel.no>

ZyXEL Spain
Tel: +34 902 195 420
Fax: +34 913 005 345
Email: sales@zyxel.es
<http://www.zyxel.es>

ZyXEL UK Ltd.
Tel: +44 (0) 1344 303044
Fax: +44 (0) 1344 303034
Email: sales@zyxel.co.uk
<http://www.zyxel.co.uk>



Copyright © 2005 ZyXEL Communications Corp. All rights reserved. ZyXEL, ZyXEL logo and ZyNOS 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.

65-100-001507G

12/05