



## Professional VPN Concentrator/UTM Appliance for SMB/Mid-Large Organizations

### Benefits

#### High-Performance VPN Concentrator Integrating Both IPSec and SSL VPN

The ZyWALL 1050 is an Internet Security Appliance engineered to provide a variety of security services on top of a robust, hardware-accelerated platform.

By integrating both IPSec VPN and SSL VPN technologies, the ZyWALL 1050 allows organizations to establish Virtual Private Network (VPN) connections amongst multiple locations such as remote branch offices, business partner sites and even remote teleworkers connected to hotel hotspots.

Since communication channels are securely encrypted, information leakage or data theft can be mitigated when transmitting confidential information over insecure networks such as Internet. In addition, the Hub and Spoke VPN feature can dramatically reduce policy management overhead in a complex, multi-site corporate network infrastructure.

#### Proactive Network Protection against Blended Threats

By integrating cutting-edge technologies on a robust platform, the ZyWALL 1050 is competent to provide multi-layered protection for security-aware businesses.

Powered by Kaspersky Labs, the gateway anti-virus security service on ZyWALL 1050 has the world's shortest response time against emerging viruses and spywares; as a result, it helps stopping blended threats on the network edge while keeping viruses/spywares out of corporate networks. With the built-in SecuASIC co-processor, the ZyWALL 1050 can still deliver robust and reliable performance even under heavy networking loads.

With the embedded signature-based IDP (Intrusion Detection and Prevention) engine, the ZyWALL 1050 performs L7 packet inspection for protocol/traffic anomaly or matched patterns to proactively provide comprehensive Intrusion Detection and Prevention capability against potential worms, viruses, Trojans horses and VoIP threats, etc.

In response to the ever-evolving threats, the ZyWALL 1050 can download the latest signature/pattern files from the rock-solid ZSDN infrastructure and install them automatically to keep itself up-to-date.

- High-Performance VPN Concentrator
- Proactive Network Protection
- IM/P2P Management
- User-Aware Policy Engine
- Bandwidth Management
- VoIP Security
- High Availability



Internet Security  
Appliance

ZyWALL 1050

## **Application Patrol to Manage the Use of IM/P2P Applications**

The ZyWALL 1050 is specially crafted to manage the use of IM/P2P applications in modern networking environments without hassle. Armed with AppPatrol, a central dashboard for managing various types of IM/P2P applications, security staff can easily create fine-grained access policies based on the ever-changing security needs: identifying and restricting different access levels of prevailing IM/P2P protocols, restricting time of access for different groups of users, enforcing bandwidth quota against certain types of P2P application and prioritizing VoIP traffics to ensure the best call quality over slow WAN ISP links. Altogether, the ZyWALL 1050 is an ideal solution to solve the dilemma in terms of productivity and security.

## **User-Aware Policy Engine Enables Access Granularity**

In addition to the basic access control capabilities, the intelligent user-aware policy engine on the ZyWALL 1050 is designed to make packet-forwarding decisions based on multiple criteria (such as user ID, user group, time of access and network quota, etc.). Furthermore, the security staff can apply access policies against a variety of security features such as VPN, Content Filter and Application Patrol.

In conjunction with VLAN and custom security zones, corporate security policies can be effectively enforced to prevent unauthorized access to the network resources.

## **Bandwidth Management Ensures Quality of Service**

The ZyWALL 1050 provides bandwidth management features for traffic prioritization to guarantee or restrict bandwidth usage per interface/protocol. Security staff can allocate bandwidth for a variety of applications or computer hosts on the corporate network, regardless of the direction of connection. For example, it's possible to assign higher priority and larger bandwidth to time-critical applications such as VoIP and video conferencing for quality transmission services. In addition, the ZyWALL 1050 allows you to keep track of bandwidth usage with comprehensive statistical reports.

## **VoIP Security: Protecting the Converged Networks**

Attracted by the benefits, more and more businesses are deploying VoIP applications on their networks. Along with the transition to VoIP also comes with security risks and voice quality issues.

As a VoIP-friendly firewall, the ZyWALL 1050 reduces the security risks associated with the adoption of VoIP by offering SIP/H.323 ALG features to dynamically open only the required ports during VoIP calls; once a call is complete, the opened ports are automatically closed to prevent port sniffing. The IDP feature can detect and prevent attacks usually associated with VoIP deployments. Ultimately, by establishing VoIP traffics over VPNs with traffic prioritization, security staff can minimize security breaches while optimizing call quality over the existing ISP links.

## **High Availability Features Guarantee Non-Stop Operations for Mission-Critical Applications**

With the High Availability features, the ZyWALL 1050 helps the security staff to easily set up a highly reliable and secure network infrastructure for your business. To minimize the impact of single-point failures, the ZyWALL 1050 supports device HA (High Availability) to assure network availability should any device failure happen.

On the WAN side, the ZyWALL 1050 can connect multiple ISP links to ensure Internet availability in case a single ISP link becomes unreliable. The multiple-WAN load-balancing feature can also optimize the bandwidth usage over each ISP link.

# Specifications

## Performance and Capacity

- SPI Firewall Throughput: 300 Mbps
- IPSec VPN (AES) Throughput: 150 Mbps
- Maximum Concurrent NAT Sessions: 128,000
- Maximum IPSec VPN Tunnels: 1,000
- Maximum SSL VPN Tunnels: 50
- New Session Rate: 10,000 (sessions/sec)

## Gateway Anti-Virus

- Stream-Based Gateway Anti-Virus Powered by Kaspersky Labs
- Covers Top Active Viruses in the Wild List
- Scans HTTP/FTP/SMTP/POP3/IMAP4
- Automatic Signature Update
- No File Size Limitation
- Blacklist/Whitelist

## Application Patrol

- IM/P2P Granular Access Control
- Integrated with Scheduling/Rate-Limit/User-Aware
- IM/P2P Up-To-Date Support\*
- Real-Time Statistical Reports

*\*: Requiring valid IDP subscription*

## Intrusion Detection and Prevention

- In-line Mode (Routing/Bridge)
- Zone-Based IDP Inspection
- Customizable Protection Profile
- Signature-Based Deep Packet Inspection
- Automatic Signature Update
- Custom Signatures
- Traffic Anomaly: Scanning Detection and Flood Protection
- Protocol Anomaly: HTTP/ICMP/TCP/UDP

## Content Filter

- URL Blocking, Keyword Blocking
- Exempt List (Blacklist and Whitelist)
- Blocks Java Applet, Cookies and Active X
- Dynamic URL Filtering Database (BlueCoat)

## VPN

### IPSec VPN (ICSA Certified)

- Encryptions (AES/3DES/DES)
- Authentication (SHA-1/MD5)
- Key Management (Manual Key/IKE)
- Perfect Forward Secrecy (DH Group 1/2/5)
- NAT over IPSec
- Dead Peer Detection/Replay Detection
- PKI (X.509)
- Certificate Enrollment (CMP/SCEP)
- Xauth Authentication
- VPN Concentrator (Hub and Spoke VPN)
- L2TP over IPSec Support

### SSL VPN

- Clientless Secure Remote Access (Reverse Proxy Mode)
- SecuExtender (Full Tunnel Mode)
- Unified Policy Enforcement
- Supports Two Factor Authentication
- Customizable User Portal

## Networking

- Routing Mode/Bridge Mode/Mixed Mode
- Layer 2 Port Grouping
- Ethernet/PPPoE/PPTP
- Tagged VLAN (802.1Q)
- Virtual Interface (Alias Interface)
- Policy-Based Routing (User-Aware)
- Policy-Based NAT (SNAT/DNAT)
- RIP v1/v2
- OSPF
- IP Multicasting (IGMP v1/v2)
- DHCP Client/Server/Relay
- Built-in DNS Server
- Dynamic DNS

## Bandwidth Management

- Bandwidth Priority
- Policy-Based Traffic Shaping
- Maximum/Guaranteed Bandwidth
- Bandwidth Borrowing

## SPI Firewall (ICSA Certified)

- Zone-Based Access Control List
- Customizable Security Zone
- Stateful Packet Inspection
- DoS/DDoS Protection
- User-Aware Policy Enforcement
- ALG Supports Custom Ports

## Authentication

- Internal User Database
- Microsoft Windows Active Directory
- External LDAP/RADIUS User Database
- ZyWALL OTP (One Time Password)
- Force User Authentication (Transparent Authentication)

## High Availability

- Device HA (Active-Passive Mode)
- Device Failure Detection
- Link Monitoring
- Auto-Sync Configurations
- Multiple WAN Load Balancing
- VPN HA (Redundant Remote VPN Gateways)

## System Management

- Role-Based Administration
- Simultaneous Administrative Logins
- Multi-Lingual Web GUI (HTTPS/HTTP)
- Object-Based Configuration

- Command Line Interface (Console/WebConsole/SSH/TELNET)
- Comprehensive Local Logging
- Syslog (4 Servers)
- E-mail Alert (2 Servers)
- SNMP v2c (MIB-II)
- Real-Time Traffic Monitoring
- System Configuration Rollback
- Text-Based Configuration File
- Firmware upgrade via FTP/FTP-TLS/WebGUI
- Advanced Reporting (Vantage Report 3.0 or above)
- Centralized Network Management (Vantage CNM 2.3/3.0\*)

*\*: Future release*

## Certifications

- ICSA Firewall Certified
- ICSA IPSec VPN Certified

## Hardware Specifications

- Memory: 512 MB RAM/256 MB Flash
- Interface: GbE x 5 (RJ-45, with LED)
- Auto-Negotiation and Auto MDI/MDI-X
- Console: RS-232 (DB9F)
- Dial Backup: RS-232 (DB9M)
- LED Indicator: PWR, SYS, ACT, HDD
- Power Switch: Yes
- Reset Pinhole: Yes
- Extension Card Slot: Yes\* (1)
- USB: Yes\* (2)
- Optional HDD: Yes\* (IDE, 2.5")

*\*: These hardware accessories will be supported in future firmware release*

## Physical Specifications

- Rack Mountable: Yes (19-inch, rack-mount kit included)
- Dimensions: 430.7 (W) x 292.0 (D) x 43.5 (H) mm
- Weight: 4,700 g

## Power Requirement

- Input voltage: 100-240 VAC, 50/60 Hz, 1 A max
- Power Rating: 80 W Max

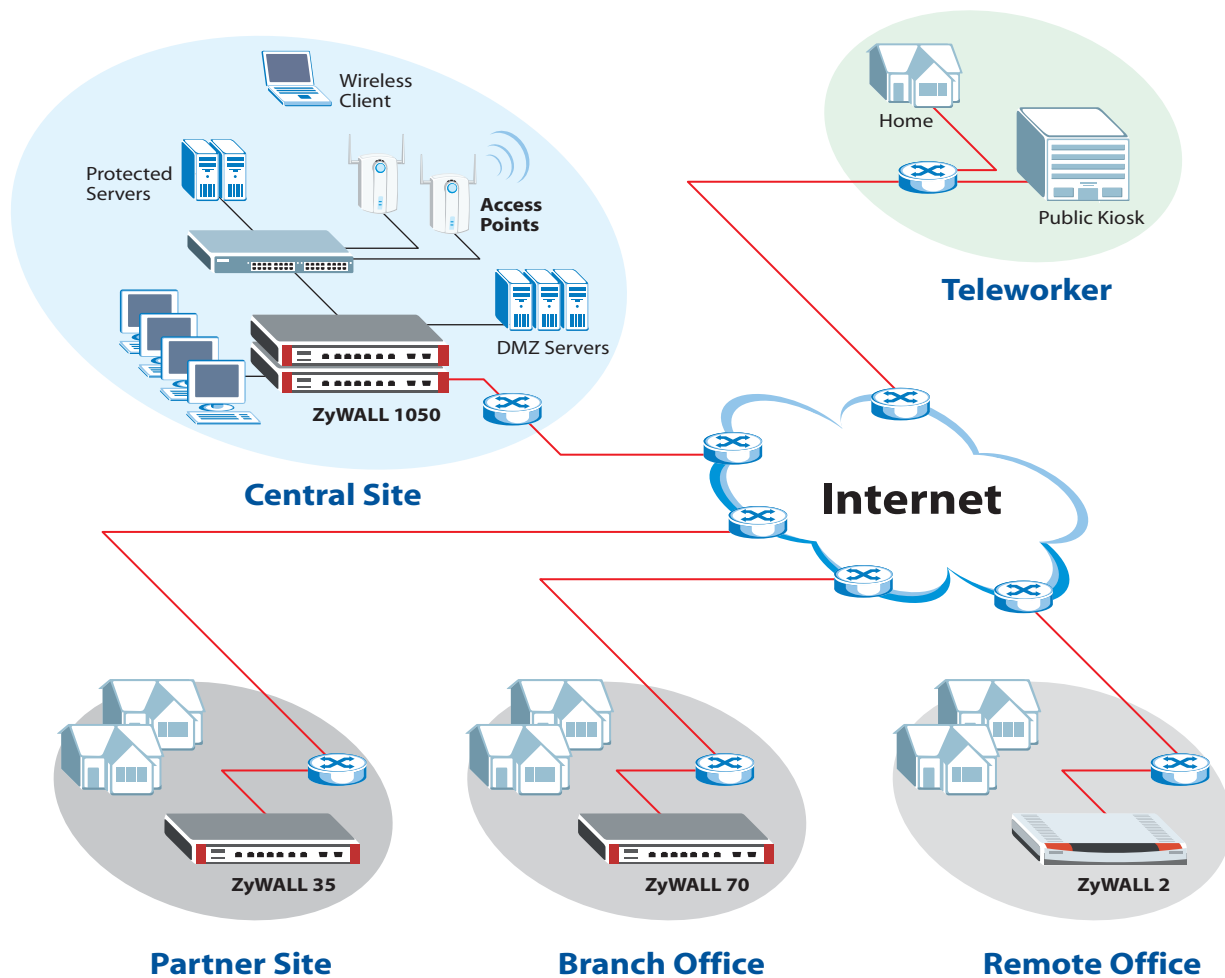
## Environmental Specifications

- Operating Temperature: 0°C ~ 40°C
- Storage Temperature: -30°C ~ 60°C
- Humidity: 5% ~ 90% (non-condensing)

## Standard Compliance

- HSF (Hazardous Substance Free): RoHS and WEEE
- EMC: FCC Part 15 Class A, CE-EMC Class A, C-Tick Class A, VCCI Class A
- Safety: CSA International (ANS/UL60950-1, CSA60950-1, EN60950-1, IEC60950-1)

## Application Diagram



Powered by Kaspersky, BlueCoat, ICSA Firewall, ICSA VPN



**Content Control**  
from **BlueCoat**



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



Copyright © 2007 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.

65-100-105002B

07/07