ZyXEL

Professional VPN Concentrator/UTM Appliance for SMB/Mid-Large Organization

Benefits

High Performance VPN Concentrator

The ZyWALL 1050 allows organizations to establish Virtual Private Network (VPN) connections among multiple locations (such as remote branch offices, business partner sites and remote teleworkers).

Data is encrypted in a VPN to secure communication channels and prevent confidential information from being eavesdropped over the Internet. Communication through VPN tunnels is protected from session hijack attacks and information theft. These security features are integrated in the ZyWALL 1050 to provide seamless data protection before transmission to a trusted network over the VPN.

The Hub and Spoke VPN feature dramatically reduces management overhead and complexity in a complex, multi-site corporate network infrastructure.

User-Aware Policy Engine Enables Access Granularity

In addition to 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.). In addition, you can apply access policies to other security features such as VPN, content filtering and application patrol.

In conjunction with network partitioning, corporate security policies can be effectively enforced to prevent unauthorized access to network or network resources.

Proactive Network Protection Mitigates Security Breaches

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

ZSRT (ZyXEL Security Response Team), ZyXEL's dedicated security experts, releases up-to-date IDP signatures/patterns in response to ever-evolving vulnerabilities/exploits. New updates are automatically downloaded and installed through ZSDN to your ZyWALL 1050.

- High performance VPN concentrator
- User-Aware policy engine
- Proactive network protection
- Robust networking functionalities
- Bandwidth management
- VoIP security
- Content filtering
- Device HA and Multiple WAN load balancing

Internet Security Appliance

ZYWALL
1050

Customizable Security Zones Deliver Flexible Policy Management

The ZyWALL 1050 supports L3 virtualization techniques (VLAN and virtual/alias interface). You can set VLAN or virtual interface to different physical ports as needed. In addition, you can group the VLANs and virtual interfaces in a zone to which consistent security policies are applied.

With the virtualization and zone concepts, the ZyWALL 1050 offers flexible deployment and easy security policy management in large/complex networking environments.

Bandwidth Management Ensures Quality of Service

ZyWALL 1050 provides the bandwidth management feature for traffic prioritization to guarantee or restrict the bandwidth usage per connection. You can allocate bandwidth to traffic types or computer hosts in the corporate network. For example, give higher priority and bigger bandwidth to time-critical applications such as VoIP and video streaming for quality transmission service. In addition, ZyWALL 1050 allows you to keep track of bandwidth usage with comprehensive centralized logs.

VoIP Security: Protecting the Converged Network

Attracted to its many benefits, more and more businesses are deploying VoIP applications in their networks. With the transition to VoIP also comes with security risks. As a VoIP-friendly firewall, the ZyWALL 1050 offers the SIP/H.323 ALG feature to dynamically open only the ports needed for the duration of the VoIP call. Once the call is complete, the ports automatically close, preventing malicious port sniffing and attacks commonly associated VoIP deployment.

Besides allowing basic VoIP functionality, the ZyWALL 1050 takes a step further to allow VoIP over VPN and provide IDP against VoIP threats for maximum security.

Employee Internet Management Increases Productivity

The content filtering feature allows schools or mid-large organizations to create and enforce Internet access policies. You can set the ZyWALL 1050 to monitor or block access based on web site categories (such as pornography or racial intolerance) from a pre-defined list. For up-to-date web site ratings, you can activate the content filtering subscription that allows the ZyWALL 1050 to query the dynamic URL database. Thus access restrictions to web sites are properly enforced and corporate policy compliance could be assured.

High Availability Features Guarantee Non-stop Operation for Mission-critical Applications

The ZyWALL 1050 supports multiple WAN ports with WAN connection backup and load balancing. In addition to WAN redundancy, the ZyWALL 1050 also supports device HA (High Availability). With these features, the ZyWALL 1050 helps you easily set up a highly reliable and secure network for your business.

Specifications

Performance and Capacity
- SPI firewall throughput: 300Mbps
- VPN AES/3DES throughput: 100Mbps
- IDP throughput: 100Mbps
- Concurrent sessions: 128,000
- New session rate: 4,000 (sessions/sec)
- Simultaneous VPN tunnels: 1,000

Security and Authentication
- DoS/DDoS prevention
- ALG supports SIP/H.323, FTP, IPSec, L2TP, MSN, PPTP and RTP
- Access granularity: ip/port/location/user/ group/time/network quota
- Customizable security zones
- Force user authentication (transparent authentication): user-aware access policy management
- User database: RADIUS, LDAP, Microsoft Active Directory and local user database
- Application Patrol: portless application management
- IM/P2P application management: blocking, scheduling, rate-limiting bandwidth
- Intrusion Detection and Prevention (inline mode or bridge mode)
- Zone-based, customizable protection profile
- Traffic anomaly for scan detection and flood detection
- Protocol anomaly: HTTP/ICMP/TCP/UDP
- Malformed packet protection
- Signature-based L3-L7 deep packet inspection
- Automatic update for latest signatures
- Custom signature supported
- VoIP over VPN
- URL blocking, keyword blocking, exempt list
- Blocks Java Applet, cookies, Active X
- URL filtering by querying dynamic database
- Gateway Anti-Virus scanning*

VPN
- Route-based IPSec VPN
- Supports Hub and Spoke VPN
- Hardware-accelerated encryption: AES, 3DES, DES
- Authentication: MD5, SHA-1
- Key management: Manual key/IKE
- PKI: PKCS #7, #10 & #12
- Certificate enrollment: CMP, SCEP
- Perfect forward secrecy: DH Group 1, 2 and 5

- NAT traversal
- NAT over IPSec
- DPD (Dead Peer Detection) and replay detection
- Split DNS tunnel
- Xauth authentication: RADIUS, LDAP, Microsoft Active Directory and local user database
- Integrated SSL VPN*

Networking
- Routing mode and bridge mode can co-exist
- Port grouping (L2)
- Supports 802.1q tagged VLAN
- Encapsulation: Ethernet/PPPoE/PPTP
- Supports virtual interface (alias interface)
- Policy-based routing
- NAT: SNAT, DNAT
- Supports dynamic routing protocols: RIP v1/v2 and OSPF
- IP Multicasting
- DHCP client/server/relay
- Built-in DNS server
- Dynamic DNS
- NTP client
- HTTP redirect
- Policy-based traffic shaping
- Maximum bandwidth
- Bandwidth priority

Redundancy
- Device HA (High Availability)
- Device failure detection
- Auto-sync configurations
- Supports multiple ISP links
- Link failure detection
- Multiple WAN load balancing
- VPN High Availability supports redundant remote VPN gateways

Management
- Intuitive Web-based GUI: https/http
- Dashboard for system status monitoring
- Role-based administration: supports multiple privileges and simultaneous logins
- Object-based architecture
- Text-based configuration file
- Full-function CLI: Accessible from console/WebConsole/ssh/telnet
- Product registration and service activation from within myZyXEL.com

- Centralized & comprehensive local logging
- Log exportable: syslog (up to 4 external syslog servers)
- SNMP v2c with MIB-II
- E-mail alert
- Real-time monitoring: Traffic snapshot and SA monitor
- Firmware upgrade: FTP, FTP-TLS, WebGUI
- System configuration rollback
- Supports Vantage Report 3.0 for advanced reporting
- Supports Vantage CNM 3.0 for centralized management

Hardware Specifications
- Memory size: 512MB system memory, 256MB onboard flash
- Five Gigabit Ethernet interfaces, RJ-45 connector with LED indicator
- Supports auto-negotiation and auto MDI/MDI-X
- RS-232, DB9F console port
- RS-232, DB9M dial backup
- LED Indicator: PWR, SYS, ACT, HDD
- Power switch and reset button
- CardBus expansion slot
- Mini-PCI expansion slot
- USB: USB 2.0 x 2 (future)
- HDD: Optional IDE, 2.5" (future)

Physical Specifications
- Rack-mountable, 19-inch
- Dimension: 430.7 (W) x 292.0 (D) x 43.5 (H) mm
- Weight: 4,700g

Power Requirement
- Input voltage: 100-240VAC, 50/60Hz, 1A max
- Power rating: 80 Watt max
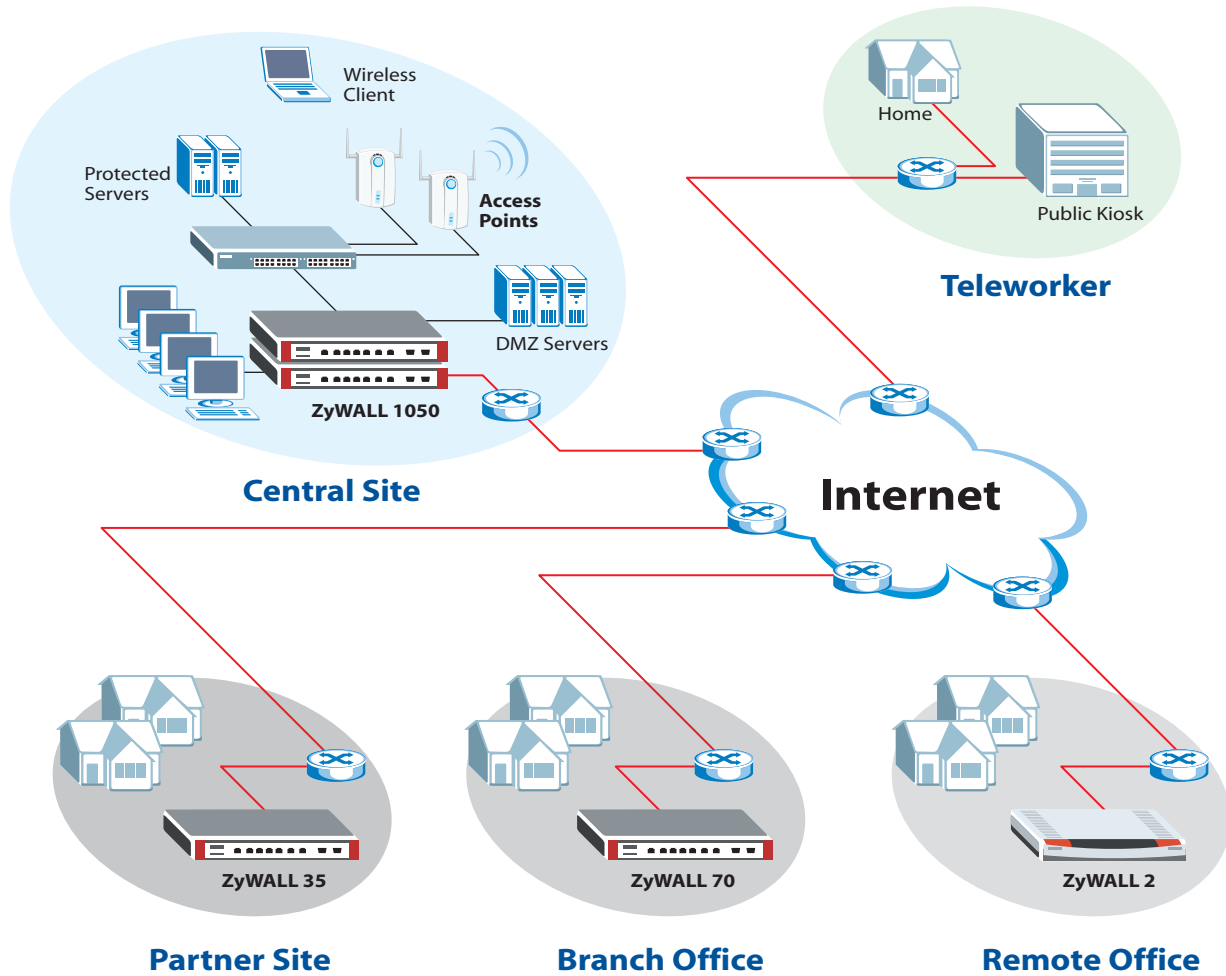
Environmental Specifications
- Operating temperature: 0ºC to 40ºC
- Operating humidity: 5% to 90% (non-condensing)

Certification
- EMC: FCC Part 15 Class A, CE-EMC Class A, C-Tick Class A, VCCI Class A
- Safety: CSA International, CE EN60950-1

Firmware upgradeable for future enhancement

Application Diagram

Central Site
- Wireless Client
- Protected Servers
- Access Points
- DMZ Servers
- ZyWALL 1050

Teleworker
- Home
- Public Kiosk

Internet

Partner Site — ZyWALL 35

Branch Office — ZyWALL 70

Remote Office — ZyWALL 2

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

65-100-974801G   06/06