Unified Security Gateway for SMB/Mid-Large Organizations

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

Internet Security Appliance

ZyWALL USG 1000

Benefits

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

ZyWALL USG 1000 is a Unified Security Gateway 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 USG 1000 allows organizations to establish Virtual Private Network (VPN) connections amongst multiple locations such as remote branch offices, business partner sites and even a remote teleworker getting connected in a potentially unsafe hotel hotspot.

Communication channels are securely encrypted so that information leakage/data theft can be mitigated when transmitting confidential information over insecure networks, such as the Internet.

The Hub and Spoke VPN feature is capable of reducing policy management overhead dramatically 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 USG 1000 is competent to provide multi-layered protection for security-aware businesses.

The gateway anti-virus security service of the ZyWALL USG 1000 is powered by Kaspersky Labs, whose technology boasts the world's shortest response time against emerging viruses and spyware. As a result, it helps stopping blended threats at the network edge while keeping viruses/spyware out of corporate networks. With a SecuASIC co-processor built-in, the ZyWALL USG 1000 can deliver robust and reliable performance under real-world networking loads.

With the embedded signature-based IDP (Intrusion Detection and Prevention) engine, the ZyWALL USG 1000 performs L7 packet inspection for protocol/traffic anomaly or matched patterns. Thus, the ZyWALL USG 1000 provides comprehensive Intrusion Detection and Prevention capability to proactively detect and block potential worms, viruses, Trojans and VoIP threats, etc.

In response to the ever-evolving threats, up-to-date signatures/patterns are automatically downloaded from rock-solid ZSDN infrastructure and installed on your ZyWALL USG 1000.

Application Patrol to Manage the Use of IM/P2P Applications

The ZyWALL USG 1000 is specially crafted to manage the use of IM/P2P applications in modern networking environment without hassles. Armed with AppPatrol, a central dashboard for managing various types of IM/P2P applications, security staff can easily create fine-grained access policy based on 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 best call quality over slow WAN ISP links. Altogether, the ZyWALL USG 1000 is an ideal solution to solve the dilemma in terms of productivity and security.

User-Aware Policy Engine Enables Access Granularity

In addition to basic access control capabilities, the intelligent user-aware policy engine on the ZyWALL USG 1000 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, 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 network resources.

Bandwidth Management Ensures Quality of Service

The ZyWALL USG 1000 provides bandwidth management features for traffic prioritization to guarantee or restrict the 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 the 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, ZyWALL USG 1000 allows you to keep track of bandwidth usage with comprehensive statistical reports.

VoIP Security: Protecting the Converged Networks

Attracted 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 USG 1000 reduces the security risks associated with the adoption of VoIP by offering the SIP/H.323 ALG feature to dynamically open only the required ports during the VoIP calls; once the call is complete, the opened ports are automatically closed to prevent port sniffing. The IDP feature can detect and prevent attacks usually associated VoIP deployment. Ultimately, by constructing VoIP traffic over VPNs with traffic prioritization, security staff could mitigate security breaches while optimizing call quality over existing ISP links.

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

With high availability features, the ZyWALL USG 1000 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 of failures, the ZyWALL USG 1000 supports device HA (High Availability) to assure network availability should any device failure happen.

On the WAN side, the ZyWALL USG 1000 can connect multiple ISP links to ensure Internet availability while a single ISP link may be unreliable. The multiple WAN load balancing features optimizes bandwidth usage over each ISP link.

Specifications

Performance and Capacity

- SPI Firewall Throughput: 350 Mbps
- IPSec VPN (AES) Throughput: 150 Mbps
- Maximum Concurrent NAT Sessions: 200,000
- Maximum IPSec VPN Tunnels: 1,000
- Maximum SSL VPN Tunnels: 50
- New Session Rate: 13,000 (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

**: Requiring valid Anti-Virus subscription*

Application Patrol (AppPatrol)

- 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

**: Requiring valid IDP subscription*

Content Filter

- URL Blocking, Keyword Blocking
- Exempt List (Blacklist and Whitelist)
- Blocks Java Applet, Cookies and Active X
- Content Filter Category Service* (Dynamic URL Filtering Database Powered by BlueCoat)

**: Requiring valid Content Filter subscription*

VPN

IPSec VPN

- 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

- 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 3.1 Patch 1*)
- Centralized Network Management (Vantage CNM 3.0*)

**: Future release*

Certifications

- ICSA Firewall Certified*
- ICSA IPSec VPN Certified*

**: Certificate pending*

Hardware Specifications

- Memory: 1GB RMB RAM/256 MB Flash
- Interface: GbE x 5 (RJ-45, with LED)
- Auto-Negotiation and Auto MDI/MDI-X
- Console: RS-232 (DB9F)
- AUX: RS-232 (DB9M)
- LED Indicator: PWR, SYS, AUX, 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 Requirements

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

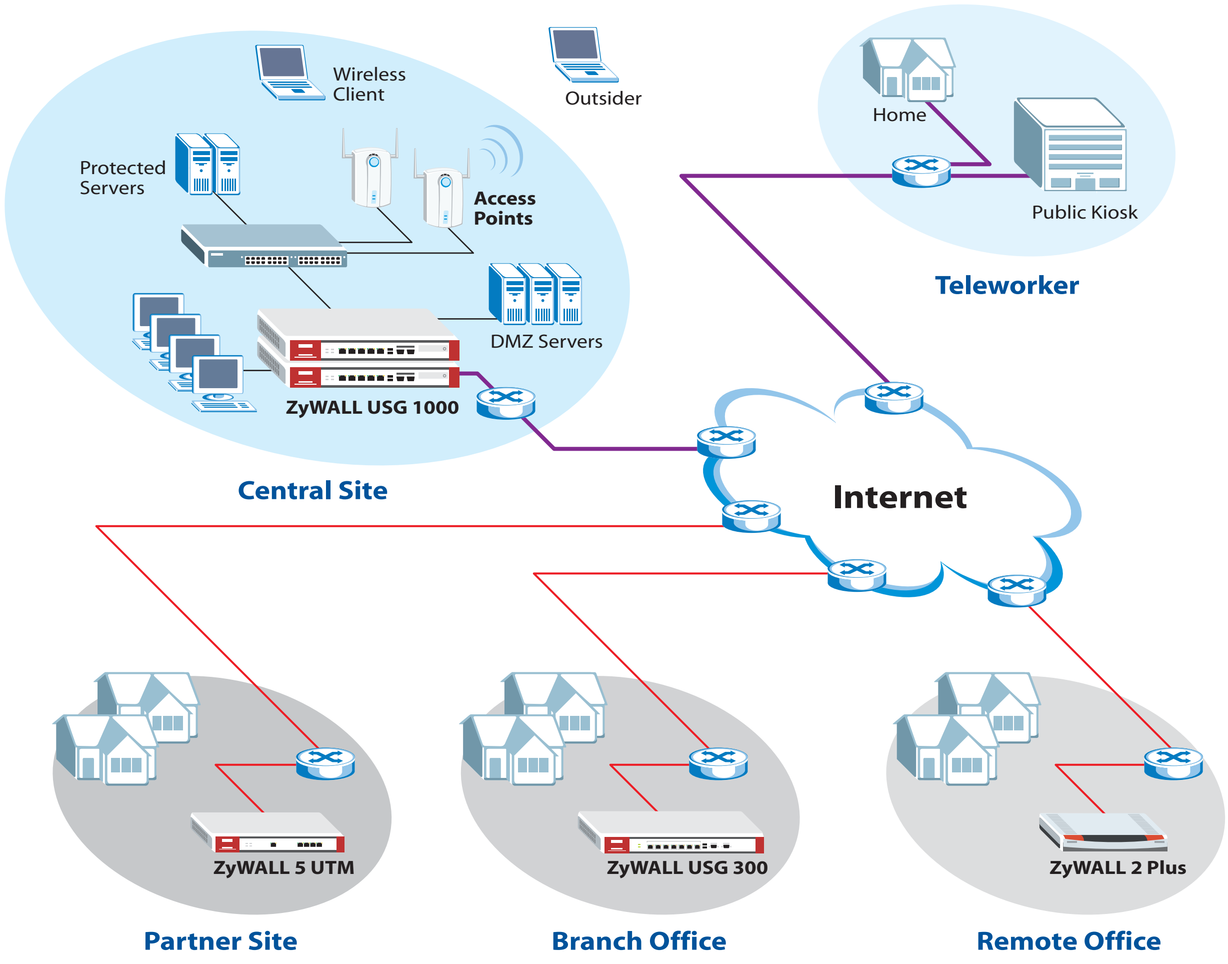
Environmental Specifications

- 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



IPSec VPN Tunnel	—
SSL VPN Tunnel	—

Powered by Kaspersky, BlueCoat, ICSA Firewall, ICSA VPN

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