ZyXEL

Unified Security Gateway for Small and Medium-Sized Businesses

- Hybrid VPN
- Comprehensive Threat Protection
- IM/P2P Management
- User-Aware Policy Engine
- Bandwidth Management
- VoIP Security
- High Availability

Internet Security Appliance

ZyWALL USG 300

Benefits

Provides IPSec VPN and SSL VPN in a Single Box

ZyWALL USG 300 is a Unified Security Gateway that integrates comprehensive enterprise-class security features tailored for SMB (Small and Medium-sized Businesses).

With streamlined integration of both IPSec VPN and SSL VPN technologies, the ZyWALL USG 300 is an ideal solution for organizations requiring intensive VPN applications across distributed networks.

No matter you are in a remote branch office or at an unreliable hotel hotspot, the ZyWALL USG 300 can establish secure communication tunnels with IPSec and/or SSL protection. Another benefit of the integration is that the user-aware access control, scheduling, bandwidth usage and anti-threat security features can be enforced against inbound and outbound traffics of the protected network resources.

Real-time Protection against Ever-Evolving Threats

By integrating cutting-edge technologies on a robust platform, the ZyWALL USG 300 is competent to provide multi-layered security for security-aware businesses.

Powered by Kaspersky Labs, the gateway anti-virus security service on ZyWALL USG 300 has the world's shortest response time against emerging viruses; as a result, it helps stopping threats on the network edge and keeps viruses/malwares out of corporate networks. With dual SecuASIC (security co-processor) built-in, the ZyWALL USG 300 can still deliver robust and reliable performance even under heavy networking loads.

In addition, the IDP feature can detect harmful attacks and take necessary actions against the malicious or suspicious activities. The signature-based IDP engine can effectively detect protocol or traffic anomalies, support behavior pattern matching and prevent malicious attacks on the application layer.

Application Patrol to Manage the Use of IM/P2P Applications

The ZyWALL USG 300 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 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 300 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 300 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 the network resources.

Bandwidth Management Ensures Quality of Service

The ZyWALL USG 300 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 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, the ZyWALL USG 300 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 USG 300 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 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 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 USG 300 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 USG 300 supports device HA (High Availability) to assure network availability should any device failure happen.

On the WAN side, the ZyWALL USG 300 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: 200 Mbps
- IPSec VPN (AES) Throughput: 100 Mbps
- Maximum Concurrent NAT Sessions: 60,000
- Maximum IPSec VPN Tunnels: 200
- Maximum SSL VPN Tunnels: 10
- New Session Rate: 2,000 (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
- 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
- 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*)
- Centralized Network Management (Vantage CNM 3.0*)

**: Future release*

Certifications
- ICSA Firewall Certified*
- ICSA IPSec VPN Certified*

**: Certificate pending*

Hardware Specifications
- Memory: 256 MB RAM/256 MB Flash
- Interface: GbE x 7 (RJ-45, with LED)
- Auto-Negotiation and Auto MDI/MDI-X
- Console: RS-232 (DB9F)
- AUX: RS-232 (DB9M)
- LED Indicator: PWR, SYS, AUX, CARD1, CARD2
- Power Switch: Yes
- Reset Pinhole: Yes
- Extension Card Slot: Yes* (2)
- USB: Yes* (2)

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

Physical Specifications
- Rack Mountable: Yes (19-inch, rack-mount kit included)
- Dimensions: 430.0 (W) x 201.2 (D) x 42.0 (H) mm
- Weight: 2,800 g

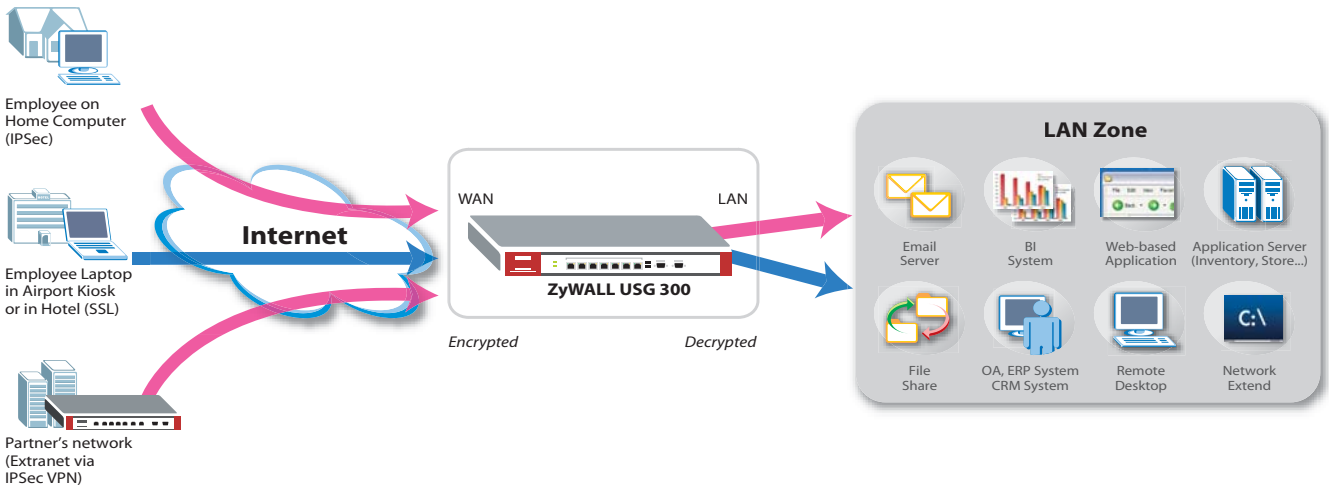
Power Requirement
- Input Voltage: 100-240 VAC, 50/60 Hz, 0.55-0.3 A
- Power Rating: 35 W Max

Environmental Specifications
- Operating Temperature: 0°C ~ 50°C
- Storage Temperature: -30°C ~ 60°C
- Humidity: 20% ~ 95% (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

Incorporates both IPSec VPN & SSL VPN into a single box



Powered by Kaspersky, BlueCoat, ICSA Firewall, ICSA VPN

Content Control from BlueCoat

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

65-100-030002G 07/07