



Unified Security Gateway, sicurezza avanzata per le SMB

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



Internet Security
Appliance

ZyWALL
USG 300

ZyXEL ZyWALL USG 300 è un Unified Security Gateway con opzioni di sicurezza avanzata per reti Small/Medium Business (SMB) fino a 200 utenti.

Le sue flessibili policy di gestione permettono agli amministratori di configurare la rete e definire le policy di sicurezza in modo più efficiente.

Il Firewall e le VPN IPSec sono certificati ICSA.

Le caratteristiche di sicurezza di ZyWALL USG 300 includono inoltre VPN SSL, Content Filter, Anti-Virus e IDP (Intrusion Detection and Prevention).

Sono inoltre previsti bandwidth management, Multiple-WAN Failover e Load Balancing.

In aggiunta gli slot di espansione permetteranno l'aggiornamento del prodotto alle nuove soluzioni tecnologiche previste in futuro.

Tramite le VPN IPSec e le VPN SSL gli utenti remoti potranno accedere ai dati aziendali in modo semplice e sicuro.

L'elevato throughput di ZyWALL USG 300 è la chiave per implementare caratteristiche di livello enterprise in un prodotto compatto che garantisce al tempo stesso servizi full time sicuri.

Vantaggi

Supporto VPN IPSec ed VPN SSL in un singolo apparato

ZyWALL USG 300 è un Unified Security Gateway, che integra caratteristiche di sicurezza di livello enterprise orientate al mercato SMB (Small and Medium-sized Businesses).

Integra sia VPN IPSec sia VPN SSL, ed è la soluzione ideale per tutte quelle organizzazioni che richiedono l'uso intensivo di applicazioni VPN su reti geografiche distribuite.

Ovunque voi siate, in un ufficio periferico o in un hot spot alberghiero, potrete stabilire un tunnel sicuro verso ZyWALL USG 300, sfruttando sia la tecnologia IPSec che SSL.

Un altro vantaggio fornito dall'apparato consiste nel fatto che le policy di sicurezza possono essere stabilite in base al tipo di connessione: controlli basati su accesso utente, o in base a schedulazione; Anti-Virus e IDP controllano il traffico entrante e uscente per proteggere le risorse di rete da eventuali attacchi.

Protezione Real-Time da virus e intrusioni

Integrando tecnologie d'avanguardia su una piattaforma hardware robusta, lo ZyWALL USG 300 è in grado di garantire sicurezza multi-livello della vostra azienda. L'Anti-Virus perimetrale di ZyWALL USG 300 è fornito da Kaspersky Labs, ed assicura i migliori tempi di risposta al mondo contro i nuovi virus.

Aiuta a bloccare le minacce e mantenere lontani virus e malware dalle risorse aziendali, bloccandoli

direttamente sul gateway. Grazie al doppio acceleratore hardware SecuASIC, l'Anti-Virus di ZyWALL USG 300 assicura performance e throughput eccellenti anche in caso di carichi di rete elevati.

Al fine di evitare problemi di sicurezza, l'IDP può rilevare attacchi nocivi e intraprendere le azioni necessarie contro le attività sospette. Le signature del motore IDP possono rilevare anomalie nei protocolli, nel traffico di rete e prevenire le intrusioni a livello applicativo. ZyWALL USG 300 è quindi una soluzione IDP completa per la sicurezza intranet ed internet.

Application Patrol per controllare l'uso delle applicazioni IM/P2P

ZyWALL USG 300 permette di bloccare l'utilizzo di instant messaging e software peer-to-peer, chiudendo potenziali back door che possono compromettere la rete, aumentando al tempo stesso la produttività e garantendo la massima banda disponibile.

Le applicazioni di instant messaging (IM) sono diventate mezzi di comunicazione aziendale sempre più diffusi e sono i bersagli favoriti dagli hackers. ZyWALL USG 300 garantisce il massimo controllo su questi programmi, i log e le statistiche dettagliate permettono agli amministratori di aumentare i controlli e la sicurezza.

Sono supportati i più importanti programmi di instant messaging come: AIM, ICQ, MSN e Yahoo Messenger.

User Aware Policy Engine per il controllo granulare degli accessi

In aggiunta alle policy di controllo di base, il motore delle policy "user-aware" permette di effettuare un controllo sul transito dei pacchetti basato su criteri multipli (user ID, user group, time access, network quota, etc.). Queste policy possono essere applicate ad altre caratteristiche di sicurezza come VPN, Firewall, Content Filter e Application Patrol.

In aggiunta alla creazione di VLAN e zone di sicurezze personalizzabili, le policy di sicurezza garantiscono una efficace prevenzione contro gli accessi non autorizzati alle risorse aziendali.

Bandwidth Management per garantire il QoS

ZyWALL USG 300 integra il bandwidth management per gestire le priorità del traffico di rete e garantire (o restringere) l'utilizzo di banda. Si può allocare banda in base al tipo di traffico o in base al computer che genera traffico. Ad esempio, si può dare una più alta priorità ed una maggiore banda alle applicazioni sensibili come il VoIP e il video streaming, per garantire la qualità del servizio. In aggiunta, ZyWALL USG 300 permette di tenere sotto controllo l'utilizzo di banda tramite log dettagliati.

Sicurezza delle comunicazioni VoIP

Molte aziende stanno integrando applicazioni VoIP all'interno della loro rete locale. Il passaggio al VoIP implica però problemi di sicurezza e di qualità legati al traffico voce.

Essendo un firewall studiato per lavorare su reti dati e voce, ZyWALL USG 300 riduce i rischi di sicurezza legati al VoIP e integra le ALG SIP/H.323 che garantiscono l'apertura dinamica delle porte necessarie alle chiamate IP; una volta terminata la chiamata VoIP queste porte vengono automaticamente chiuse sul firewall al fine di evitare buchi di sicurezza.

L'IDP può individuare e prevenire gli attacchi associati al VoIP, stabilendo comunicazioni VoIP su VPN con le relative priorità associate al traffico voce, lo staff IT può ridurre al minimo i rischi di sicurezza ottimizzando la qualità delle chiamate, sfruttando la connessione internet già esistente.

Supporto HA per evitare il Single Point of Failure

Grazie alle caratteristiche di alta affidabilità, ZyWALL USG 300 permette di configurare semplicemente una infrastruttura di rete sicura e ridondata. Per minimizzare l'impatto del Single Point of Failure, ZyWALL USG 300 fornisce il supporto HA (High Availability) per assicurare un aggiornamento hardware dell'apparato in caso di rottura. Lato WAN, ZyWALL USG permette di gestire collegamenti ISP multipli in modo da garantire la disponibilità di Internet nel caso di perdita di un link. In aggiunta è possibile gestire il load balancing per ottimizzare l'utilizzo di banda su ogni collegamento WAN.

Specifiche Tecniche

Prestazioni e Capacità

- Throughput SPI firewall: 200Mbps
- Throughput VPN AES/3DES: 100Mbps
- Throughput UTM: 48Mbps
- Sessioni NAT contemporanee: 60,000
- Nuove sessioni NAT al secondo: 2,000 (sessions/sec)
- Tunnel VPN IPSec simultanei: 200

Sicurezza ed Autenticazione

- Motore Anti-Virus stream-based (fornito da Kaspersky Labs)
- Scansione dei protocolli HTTP/SMTP/POP3/IMAP4/FTP
- Update automatico delle signature Anti-Virus
- Nessuna limitazione sulla dimensione dei file da scansionare
- Blacklist/Whitelist
- Prevenzione da attacchi DoS/DDoS
- Supporto ALG SIP/H.323, FTP, IPSec, L2TP, MSN, PPTP ed RTP
- Controllo granulare degli accessi: ip/port/location/user/group/time/network quota
- Zone di sicurezza personalizzabili
- Forzatura dell'autenticazione utente
- Database utenti: RADIUS, LDAP, Microsoft Active Directory e database utenti locale
- Application Patrol: gestione portless delle applicazioni
- Gestione delle applicazioni IM/P2P: blocco, schedulazione, limitazione della banda
- Intrusion Detection and Prevention (inline mode o bridge mode)
- Zone-based, profili di protezione personalizzabili
- Controllo delle anomalie del traffico (scan detection e flood detection)
- Controllo delle anomalie dei protocolli: HTTP/ICMP/TCP/UDP
- Protezione contro i pacchetti malformati
- Ispezione dei pacchetti L3-L7 signature-based
- Update automatico delle signature IDP
- Signature IDP personalizzabili
- VoIP su VPN
- Blocco degli URL e delle keyword, Blacklist/Whitelist
- Blocco di Java Applet, cookies ed Active X
- Filtro URL utilizzando il database esterno di BlueCoat

VPN (ICSA IPSec Certified)

- IPSec VPN route-based
- Encryption con accelerazione hardware: AES, 3DES, DES
- Authentication: MD5, SHA-1
- Gestione chiavi d'autenticazione: Manual key/IKE
- PKI: PKCS #7, #10 & #12

- Sottoscrizione dei certificati: CMP, SCEP
- Perfect forward secrecy: DH Group 1, 2 and 5
- NAT traversal
- NAT over IPSec
- DPD (Dead Peer Detection) e replay detection
- Split DNS tunnel
- Xauth authentication: RADIUS, LDAP, Microsoft Active Directory e database utenti locale
- SSL VPN integrate
- Accesso remoto sicuro clientless
- SecuExtender: supporto di qualsiasi applicazione su VPN SSL
- Supporto autenticazione RADIUS, LDAP, Microsoft Active Directory e database utenti locale
- Supporto ZyWALL OTP (One Time Password)

Networking

- Routing mode e bridge mode possono essere utilizzati contemporaneamente
- Port grouping (L2)
- Supporto VLAN 802.1q
- Encapsulation: Ethernet/PPPoE/PPTP
- Supporto virtual interface (alias interface)
- Routing policy-based
- NAT: SNAT, DNAT
- Supporto dei protocolli di routing dinamici: RIP v1/v2 and OSPF
- IP Multicasting
- DHCP client/server/relay
- DNS server integrato
- Dynamic DNS
- NTP client
- HTTP redirect
- Traffic shaping policy-based
- Limitazione dell'utilizzo di banda
- Gestione delle priorità di banda

Ridondanza

- Device HA (High Availability)
- Individuazione della rottura dell'apparato in HA
- Auto sincronizzazione degli apparati in HA
- Supporto di link ISP multipli
- Load balancing su WAN multiple
- VPN High Availability con supporto dei gateway VPN ridondati

Gestione

- Web-based GUI di semplice utilizzo: https/http
- Dashboard per il monitoraggio dell'apparato
- Amministrazione role-based: supporto privilegi utente multipli con login simultanei
- Architettura object-based
- File di configurazione text-based
- CLI full-function: accessibile da console/WebConsole/ssh/telnet

- Registrazione prodotto e attivazione servizi su myZyXEL.com
- Logging locale centralizzato e dettagliato
- Log esportabili: fino a 4 syslog server esterni
- SNMP v2c con MIB-II
- E-mail alert
- Monitoraggio real-time: traffic snapshot e SA monitor
- Firmware upgrade: FTP, FTP-TLS, WebGUI
- Possibilità di salvare in memoria più file di configurazione
- Supporto per il Vantage Report 3.1* per reportistica avanzata
- Supporto per il Vantage CNM 3.0* per il management centralizzato

*: Future release

Certificazioni

- Firewall certificato ICSA *
- IPSec certificato ICSA *
- IPS certificato ICSA *

*: in attesa

Specifiche Hardware

- Memoria: 256MB di memoria di sistema, 256MB flash
- GbE x 7, connettori RJ-45 (con LED), auto-negoziante e auto MDI/MDI-X
- RS-232, porta console DB9F
- RS-232, dial backup DB9M
- Indicatori LED: PWR, SYS, AUX, CARD1, CARD2
- Pulsante di spegnimento e pulsante di reset
- Slot di espansione*: CardBus slot x 2
- USB*: USB 2.0 x 2

* Release firmware future

Specifiche fisiche

- Rack-mountable, 19-pollici, 1U
- Dimensioni: 430.0(L) x 201.2(P) x 42.0(A) mm
- Peso: 2,800g
- MTBF: 180382 ore

Alimentazione

- Voltaggio: 100-240VAC, 50/60Hz, 0.55-0.3A
- Potenza: 35 Watt max

Specifiche ambientali

- Temperature utilizzo: da 0 °C a 50 °C; umidità: 20% a 95% (non-condensing)
- Temperature ambiente: -30 °C a 60 °C; umidità: 20% a 95% (non-condensing)

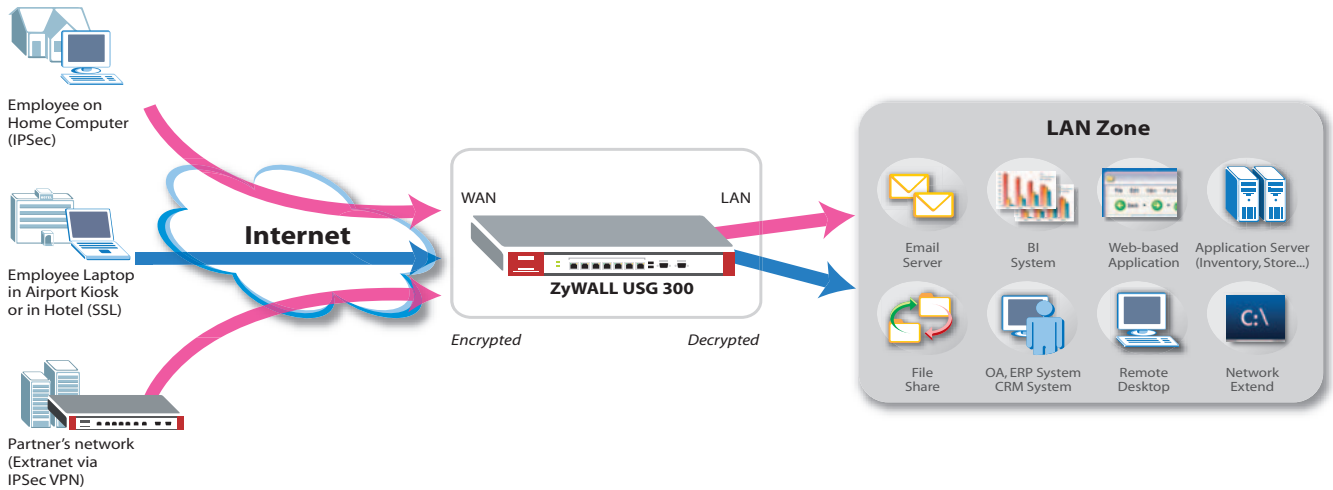
Certificazioni

Rispetta gli standard

- 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, CE EN60950-1 (UL60950-1)

Applicazioni

Include VPN IPSec & SSL



Powered by Kaspersky, BlueCoat, ICSA Firewall, ICSA VPN



Content Control
from **BlueCoat**



Per maggiori informazioni: www.ZyXEL.it



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.