ZyXEL

Passerelle de Sécurité Unifiée pour Petites et Moyennes Entreprises

- VPN Hybride
- Protection Compréhensive des menaces
- Gestion IM/P2P
- Appareil de sécurité User-Aware
- Gestion de la bande passante
- Securité VoIP
- Haute disponibilité

Appliance
Securité Internet

ZyWALL
USG 300

Avantages

Fournit le VPN IPSec et SSL VPN dans un même appareil

Le ZyWALL USG 300 est une passerelle de sécurité unifiée qui intègre les caractéristiques de sécurité créées pour les PME (Petites et Moyennes Entreprises).

Avec l'intégration des deux technologies VPN, IPSec et SSL, le ZyWALL USG 300 représente une solution idéales pour les entreprises nécessitant des applications VPN sur des réseaux distribués.

Que vous vous trouviez dans une filiale ou sur un hotspot d'hôtel non relié, le ZyWALL USG 300 peut établir des tunnels de communication sécurisés avec la protection IPSec et/ou SSL. Un autre avantage de l'intégration est que le contrôle d'accès user-aware, le scheduling, l'usage de la bande passante et la sécurité anti-menaces peuvent être renforcés contre les trafics entrants et sortants des ressources protégées du réseau.

Protection en temps réel contre les menaces en perpétuelle évolution

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 pour gérer l'utilisation des applications IM/P2P

Le ZyWALL USG 300 est spécialement conçu pour gérer sans problème l'utilisation d'applications IM/P2P dans des environnements réseau modernes. Armé de l' AppPatrol, un tableau de bord central pour la gestion de types variés d'applications IM/P2P, l'équipe de sécurité peut facilement créer des polices d'accès granulées finement, basées sur les besoins de sécurité en changement perpétuel : identifier et restreindre différents niveaux d'accès des protocoles IM/P2P dominants, restreindre le temps d'accès pour différents groupes d'utilisateurs, renforcer le quota de bande passante contre certains types d'applications P2P et prioriser les trafics VoIP pour assurer la meilleure qualité vocale sur des liens ISP WAN lents. Le ZyWALL USG 300 est une solution idéale pour résoudre le dilemme en terme de productivité et de sécurité.

Appareil de police de sécurité “User-Aware” permettant la granularité d’accès

En plus des capacités de contrôle d’accès de base, l’appareil de polices de sécurité intelligent « user-aware » du ZyWALL USG 300 est conçu pour prendre des décisions de transfert de paquets selon des critères multiples (tels que l’identification de l’utilisateur, le groupe d’utilisateurs, l’heure de l’accès et le quota de réseau, etc…). en outre, l’équipe de sécurité peut appliquer les polices de sécurité selon une variété de caractéristiques de sécurité telles que le VPN, le filtrage de contenu et l’ Application Patrol.

En union avec les zones de sécurité VLAN et client, les polices de sécurité de l’entreprise peuvent être renforcées efficacement pour bloquer l’accès non autorisé aux ressources du réseau.

Gestion de la bande passante pour garantir la qualité de service

Le ZyWALL USG 300 fournit des caractéristiques de gestion de bande passante pour la priorisation du trafic, afin de garantir ou de restreindre l’usage de bande passante par interface/protocole.

L’équipe de sécurité peut allouer la bande passante pour une variété d’applications ou pour les ordinateurs hôtes sur le réseau de l’entreprise, sans tenir compte de la direction de la connexion.

Par exemple, il est possible d’assigner une plus forte priorité et une plus grande passante à des applications sensibles en temps telles que la VoIP et la vidéoconférence, afin de garantir la qualité des services de transmission. En plus, le ZyWALL USG 300 vous permet de conserver une trace de l’utilisation de la bande passante avec des rapports statistiques compréhensifs.

Sécurité VoIP : protection des réseaux convergents

Attirés par les avantages, de plus en plus d’entreprises déploient des applications VoIP sur leurs réseaux. Avec la transition vers la VoIP, surgissent des risques de sécurité et des problèmes de qualité de la voix.
Conçu pour supporter la VoIP, le firewall ZyWALL USG 300 réduit les risques de sécurité associés à l’adoption de la VoIP en offrant la caractéristique SIP/H.323 ALG pour ouvrir dynamiquement les ports nécessaires pendant les appels VoIP ; lorsque les appels sont terminés, les ports ouverts sont fermés automatiquement pour éviter le port sniffing.
La caractéristique IDP peut détecter et éviter les attaques habituellement associées aux déploiements VoIP. Finalement, en établissant des trafics VoIP sur des VPN avec priorisation de trafic, l’équipe de sécurité peut réduire les failles de sécurité en optimisant la qualité des appels sur les liens ISP existants.

Caractéristiques High Availability garantissant les fonctionements non-stop pour les applications de missions critiques

Avec les caractéristiques High Availability, le ZyWALL USG 300 aide l’équipe de sécurité à paramétrer facilement une infrastructure fiable et sécurisée pour votre entreprise. Pour réduire l’impact d’erreurs sur un seul point, le ZyWALL USG 300 supporte le HA (High Availability) appareil pour garantir la disponibilité du réseau même si l’appareil devait montrer un défaut.

Sur le côté WAN, le ZyWALL USG 300 peut se connecter sur de multiples liens ISP pour assurer la disponibilité de l’Internet au cas où un seul lien ISP devait être indisponible. La caractéristique d’équilibrage de charge multiple WAN peut également optimiser l’utilisation de bande passante sur chaque lien ISP.

Spécifications

Performance et Capacité
- Débit Firewall SPI : 200 Mbps
- Débit VPN IPSec (AES) : 100 Mbps
- Sessions NAT concurrentes maximum : 60,000
- Tunnels VPN IPSec maximum : 200
- Tunnels VPN SSL maximum : 10
- Taux de nouvelles sessions : 2,000 (sessions/sec)

Passerelle Anti-Virus
- Passerelle anti-virus basée sur le flux fournie by Kaspersky Labs
- Couvre les virus top actifs dans la Wild List
- Scane HTTP/FTP/SMTP/POP3/IMAP4
- Mise à jour automatique des signatures
- aucune limitation de taille de fichier Fil
- Blacklist/Whitelist

Application Patrol
- contrôle d'accès granulaire IM/P2P
- Integré avec Scheduling/Rate-Limit/ User-Aware
- Support toujours actuel IM/P2P*
- Rapports statistiques en temps réel

**:Nécesstite une souscription IDP valide*

Détection et prévention d'intrusion
- In-line Mode (Routing/Bridge)
- Inspection IDP basée sur la zone
- Profil de protection personnalisable
- Inspection Deep Packet basée sur la signature
- Mises à jour automatique des signatures
- Custom Signatures
- Anomalie de trafic : Scanning Detection and Flood Protection
- Anomalie de protocole : HTTP/ICMP/TCP/UDP

Filtrage du contenu
- Blocage d'URL, blocage par mot clé
- Liste Exempt (Blacklist et Whitelist)
- Bloque Java Applet, Cookies et Active X
- Base de donnée filtrage URL dynamique (BlueCoat)

VPN
VPN IPsec
- Chiffrements (AES/3DES/DES)
- Authentification (SHA-1/MD5)
- Gestion de clé (Clé manuelle/IKE)
- Perfect Forward Secrecy (DH Group 1/2/5)
- NAT over IPSec
- Dead Peer Detection/Replay Detection
- PKI (X.509)
- Certificate Enrollment (CMP/SCEP)
- Authentification Xauth
- Support L2TP over IPSec

VPN SSL
- Accès distant sécurisé sans client (Reverse Proxy Mode)
- SecuExtender (Full Tunnel Mode)
- Renforcement de la sécurité unifiée
- Supporte l'authentification Two Factor
- Portail d'utilisateur personnalisable

Réseau
- Mode routage / mode bridge /Mode mixte
- Groupage de port couche 2
- Ethernet/PPPoE/PPTP
- VLAN tagué (802.1Q)
- Interface virtuelle (Interface Alias)
- Routage basé sur la police de sécurité (User-Aware)
- NAT basé sur la police de sécurité (SNAT/DNAT)
- RIP v1/v2
- OSPF
- IP Multicasting (IGMP v1/v2)
- DHCP Client/Serveur/Relais
- Serveur DNS intégré
- DNS Dynamique

Gestion de la bande passante
- Priorité de bande passante
- Traffic Shaping basé sur la police de sécurité
- Bande passante maximale/garantie
- Emprunt de bande passante

Firewall SPI
- Liste de contrôle d'accès basée sur la zone
- Zone de sécurité personnalisable
- Stateful Packet Inspection
- Protection DoS/DDoS
- Renforcement de la sécurité « User-Aware »
- ALG Supports Custom Ports

Authentification
- Base de données utilisateurs interne
- Microsoft Windows Active Directory
- Base de données utilisateurs externe LDAP/RADIUS
- ZyWALL OTP (One Time Password)
- Authentification d'utilisateur forcée (authentification transparent)

Haute disponibilité
- HA appareil (Active-Passive Mode)
- Détection d'erreur appareil
- Link Monitoring
- Configurations Auto-Sync
- Equilibrage de charge Multiple WAN
- VPN HA (passerelles VPN distantes redondantes)

Administration du système
- Administration basée sur le rôle
- Logins administrateur multiples
- Interface web GUI multilingue (HTTPS/HTTP)
- Configuration basée sur l'objet
- Interface ligne de commandes (Console/WebConsole/SSH/TELNET)
- Logging local compréhensif
- Syslog (4 serveurs)
- Alerte par email (2 serveurs)
- SNMP v2c (MIB-II)
- Contrôle du trafic en temps réel
- Retour à l'ancienne Configuration Système
- Fichier de configuration basé sur le texte
- Mise à jour de firmware via FTP/FTP-TLS/Web GUI
- Reporting avancé (Vantage Report 3.1*)
- Centralized Network Management (Vantage CNM 3.0*)

**: Mise à jour future*

Certifications
- Firewall certifié ICSA*
- VPN certifié ICSA IPSec*

**: Selon le certificat*

Spécifications matérielles
- Mémoire : 256 MB RAM/256 MB Flash
- Interface : GbE x 7 (RJ-45, avec LED)
- Auto-Negotiation et Auto MDI/MDI-X
- Console : RS-232 (DB9F)
- AUX : RS-232 (DB9M)
- Indicateurs LED : PWR, SYS, AUX, CARD1, CARD2
- Power Switch: Oui
- Reset Pinhole: Oui
- Slot pour carte d'extension : Oui* (2)
- USB : Oui* (2)

**:Ces accessoires matériels seront supportés par mise à jour future de firmware*

Spécifications physiques
- Rackable : Oui (19-inch, kit de montage inclus)
- Dimensions : 430.0 (L) x 201.2 (l) x 42.0 (h) mm
- Poids : 2,800 g

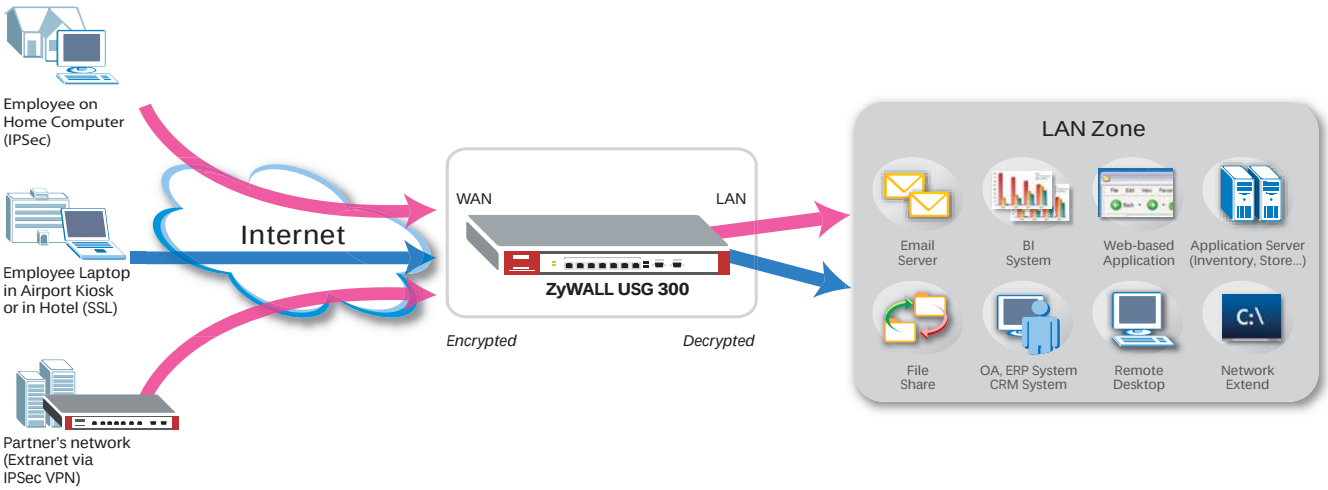
Alimentation
- Voltage entrée: 100-240VAC, 50/60 Hz, 0.55-0.3A
- Alimentation : 35 W Max

Spécifications environnementales
- Température d'exploitation : 0°C ~ 50°C
- Température de stockage : -30°C ~ 60°C
- Humidité : 20% ~ 95% (sans condensa)

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

Diagramme d'Application

Intègre le VPN IPSec & le VPNSSL dans un même appareil



Powered by Kaspersky, BlueCoat, ICSA Firewall, ICSA VPN

Pour plus d'informations sur les produits, visitez notre site web sur w w w. Z y X E L .com

65-100-030002G 07/07