ZyXEL

Concentrateur VPN professionnel/application UTM pour PME et entreprises de taille moyenne

- Concentrateur VPN haute performance
- Moteur de règles tenant compte de l'utilisateur
- Protection proactive du réseau
- Fonctionnalités réseau robustes
- Gestion de la bande passante
- Sécurité VoIP
- Filtrage de contenus
- Équilibrage de charge par périphérique HA (grande disponibilité) et réseau étendu multiple

Internet en toute sécurité

ZyWALL 1050

Points forts

Concentrateur VPN haute performance

Le ZyWALL 1050 permet aux entreprises de mettre en place des connexions de réseau privé virtuel (VPN) entre plusieurs sites, tels que les bureaux à distance, les sites partenaires ou les télétravailleurs.

Les canaux de communication sont sécurisés grâce à l'encryptage des données dans un VPN, empêchant les informations confidentielles d'être interceptées sur Internet. Les communications via les tunnels VPN sont ainsi protégées du piratage et du vol d'informations. Ces caractéristiques de sécurité intégrées au ZyWALL 1050 permettent une protection sans faille des données avant que celles-ci ne soient transmises à un réseau de confiance via le VPN.

La fonction VPN « hub and spoke » réduit grandement la surcharge et la difficulté de gestion d'une infrastructure réseau complexe et sur plusieurs sites.

Le moteur de règles tenant compte de l'utilisateur permet la granularité des accès

Outre ses capacités de contrôle des accès de base, le moteur de règles intelligent du ZyWALL 1050, qui tient compte de l'utilisateur, a été conçu pour prendre des décisions de transmission des paquets en s'appuyant sur plusieurs critères (ID ou groupe d'utilisateur, heure d'accès, quota du réseau, etc.). De plus, vous pouvez appliquer les règles d'accès à d'autres caractéristiques de sécurité telles que le VPN, le filtrage des contenus et l'application Patrol.

Associées à la segmentation du réseau, les règles de sécurité de l'entreprise peuvent être efficacement appliquées afin d'empêcher les accès non autorisés au réseau ou à ses ressources.

La protection proactive du réseau réduit les failles de sécurité

Grâce à la fonction intégrée de détection et de prévention des intrusions basée sur les signatures, le ZyWALL 1050 effectue une inspection des paquets de niveau 7 à la recherche d'anomalies de protocole ou de formes associées. Il offre ainsi une détection et une prévention complètes des intrusions et permet de déceler et de bloquer de façon proactive les vers, virus, chevaux de Troie et autres menaces VoIP potentielles.

Les experts en sécurité de la ZSRT (ZyXEL Security Response Team) élaborent des signatures et des formes IDP actualisées en réponse à l'évolution constante des menaces et des applications. Les mises à jour sont automatiquement téléchargées et installées sur votre ZyWALL 1050 via le ZSDN (réseau de distribution sécurisée).

Les zones de sécurité personnalisables facilitent la gestion des règles

Le ZyWALL 1050 est compatible avec les techniques de virtualisation de niveau 3 (VLAN et interface virtuelle/alias). Vous pouvez installer un VLAN ou une interface virtuelle sur différents ports physiques en fonction de vos besoins. Vous avez également la possibilité de regrouper les VLAN et les interfaces virtuelles dans une zone soumise à des règles de sécurité homogènes.

Grâce aux systèmes de virtualisation et de zones, le ZyWALL 1050 permet un déploiement souple et une gestion facilitée des règles de sécurité dans des environnements réseau vastes ou complexes.

La gestion de la bande passante garantit la qualité du service

Grâce à ses caractéristiques de priorisation du trafic, le ZyWALL 1050 garantit ou limite l'utilisation de la bande passante à chaque connexion. Vous pouvez ainsi allouer une bande passante à certains types de trafic ou à des ordinateurs hôtes du réseau de l'entreprise en accordant, par exemple, une priorité et une bande passante plus élevées à certaines applications exigeantes telles que le VoIP ou la lecture de fichiers vidéo pour une excellente transmission. De plus, le ZyWALL 1050 vous permet de garder des traces de l'utilisation de la bande passante à l'aide de journaux centralisés et complets.

La sécurité VoIP protège le réseau convergent

Attirées par les nombreux avantages des applications VoIP, de plus en plus d'entreprises en déploient sur leurs réseaux. Mais la migration vers la VoIP comporte également certains risques en termes de sécurité.

Pare-feu adapté à la VoIP, le ZyWALL 1050 est équipé d'une passerelle d'application SIP/H.323 afin d'ouvrir uniquement, et de façon dynamique, les ports nécessaires pendant la durée de l'appel VoIP.

Une fois l'appel terminé, les ports se ferment automatiquement, empêchant ainsi tout repérage ou attaque fréquemment associés au déploiement VoIP.

Outre la fonction VoIP de base, le ZyWALL 1050 détecte et prévient les intrusions et permet d'utiliser la technologie VoIP via un VPN pour une sécurité maximale.

La gestion Internet des employés augmente la productivité

Le filtrage de contenus permet aux écoles ou aux entreprises de taille moyenne de créer et de mettre en place des règles d'accès à Internet. Il est ainsi possible de paramétrer le ZyWALL 1050 pour surveiller ou bloquer les accès à certaines catégories de sites Internet (pornographie ou racisme p. ex.) à partir d'une liste prédéfinie. La souscription au filtrage de contenus, qui permet au ZyWALL 1050 de se connecter à la base de données dynamique des URL, peut être activée pour obtenir les classements actualisés des sites Internet. La restriction des accès à certains sites et les règles de l'entreprise s'en trouvent ainsi respectées.

Les caractéristiques de grande disponibilité garantissent une exploitation continue pour les applications vitales

Le ZyWALL 1050 est compatible avec des ports WAN multiples pour la sauvegarde et l'équilibrage de charge des connexions WAN. Outre la redondance du réseau étendu, il supporte également les périphériques HA (grande disponibilité). Grâce à ses caractéristiques, le ZyWALL 1050 vous aide à installer facilement un réseau très fiable et sécurisé dans votre entreprise.

Spécifications

Performances et capacités
- Débit pare-feu SPI : 300 Mbps
- Débit VPN AES/3DES : 100 Mbps
- Débit IDP : 100 Mbps
- Sessions concurrentes : 128 000
- Taux de nouvelles sessions : 4000 (sessions/sec)
- Tunnels VPN simultanés : 1000

Sécurité et authentification
- Prévention des attaques de type DoS/DDoS
- Compatibilité de la passerelle d'application avec les fonctions SIP/H.323, FTP, IPSec, L2TP, MSN, PPTP et RTP
- Granularité d'accès : IP/port/site/utilisateur/groupe/heure/quota du réseau
- Zone de sécurité personnalisable
- Authentification de l'utilisateur (transparente) : gestion des règles d'accès tenant compte de l'utilisateur
- Base de données utilisateurs : RADIUS, LDAP, Microsoft Active Directory et base de données de l'utilisateur local
- Application Patrol : gestion des applications sans port
- Gestion des applications IM/P2P : blocage, programmation, limitation des taux de bande passante
- Détection et prévention des intrusions (mode linéaire ou pont)
- Profil de protection basé sur des zones et personnalisable
- Anomalies du trafic pour la détection des scans et des inondations
- Anomalie de protocole : HTTP/ICMP/TCP/UDP
- Protection contre les paquets mal formés
- Inspection approfondie des paquets de niveau 3 à 7 basée sur la signature
- Mise à jour automatique des signatures les plus récentes
- Compatible avec les signatures personnalisées
- VoIP via VPN
- Blocage d'URL et de mots-clés, liste d'exceptions
- Blocage des applications Java, des cookies et d'Active X
- Filtrage URL après interrogation de la base de données dynamique
- Analyse anti-virus de la passerelle*

VPN
- VPN IPSec basé sur route
- Compatibilité « hub and spoke » VPN
- Encryptage accéléré sur disque dur : AES, 3DES, DES
- Authentification : MD5, SHA-1
- Gestion des clés : gestion manuelle des clés/IKE
- PKI : PKCS #7, #10 & #12
- Inscription des certificats : CMP, SCEP
- Transmission parfaitement confidentielle : DH Group 1, 2 et 5
- NAT Tranversal
- NAT via IPSec
- DPD (Dead Peer Detection) et détection de répétition
- Tunnel DNS partagé
- Authentification Xauth : RADIUS, LDAP, Microsoft Active Directory et base de données de l'utilisateur local
- VPN SSL intégré*

** Possibilité de mise à jour du microprogramme pour les versions ultérieures*

Réseau
- Coexistence possible entre les modes routage et pontage
- Groupage de ports (niveau 2)
- Compatibilité marquage VLAN (802.1q)
- Encapsulation : Ethernet/PPPoE/PPTP
- Compatibilité interface virtuelle (interface alias)
- Règles de routage
- NAT : SNAT, DNAT
- Compatibilité protocoles de routage dynamiques : RIP v1/v2 et OSPF
- Multicasting IP
- Serveur/relais/client DHCP
- Serveur DNS intégré
- DNS dynamique
- Client NTP
- Redirection HTTP
- Règles de lissage du trafic
- Bande passante maximum
- Priorité de la bande passante

Redondance
- Périphériques HA (grande disponibilité)
- Détection des défaillances des périphériques
- Configurations avec synchronisation automatique
- Compatibilité avec liens FAI multiples
- Détection des défaillances des liens
- Équilibrage de charge sur réseau étendu multiple
- Grande disponibilité VPN compatible avec les passerelles VPN éloignées et redondantes

Gestion
- Interface graphique intuitive basée sur le Web : http/https
- Outil de surveillance du statut du système
- Administration basée sur la fonction : privilèges multiples et logins simultanés
- Architecture basée sur les objets
- Fichier de configuration en mode caractère
- Fonction ILC complète, accès console/ console Web/ssh/telnet
- Enregistrement du produit et activation du service depuis myZyXEL.com
- Login local centralisé et complet
- Journal exportable : syslog (jusqu'à 4 serveurs syslog externes)
- SNMP v2c avec MIB-II
- Alertes par e-mail
- Surveillance en temps réel : photo du trafic et moniteur SA
- Mise à jour du microprogramme : FTP, FTP-TLS, interface graphique basée sur le Web
- Rollback de la configuration du système
- Compatible avec le Vantage Report 3.0 pour le reporting avancé
- Compatible avec le Vantage CNM 3.0 pour la gestion centralisée

Matériel
- Mémoire vive : 512 Mo de mémoire système, 256 Mo flash onboard
- Cinq interfaces Ethernet Gigabit, connecteur RJ-45 avec indicateur DEL
- Négociation et MDI/MDI-X automatiques
- RS-232, port console DB9F
- RS-232, sauvegarde de la numérotation DB9M
- Voyant DEL : PWR, SYS, ACT, HDD
- Interrupteur et bouton reset
- Connecteur d'extension CardBus
- Connecteur d'extension Mini-PCI
- USB : 2 ports USB 2.0 (futur)
- HDD : IDE optionnel, 2,5" (futur)

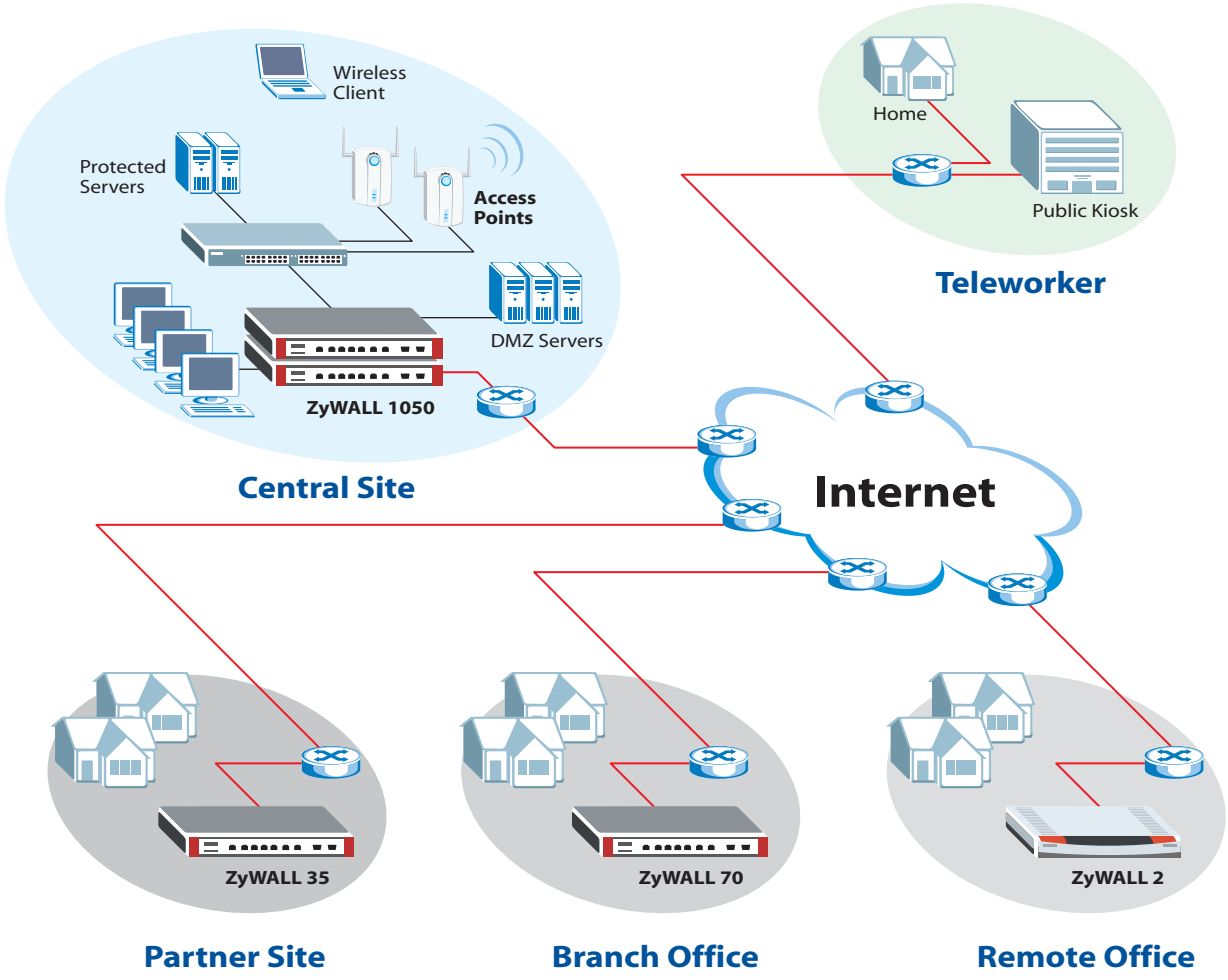
Dimensions & poids
- Montable sur rack, 19 pouces
- Dimensions: 430,7mm(L) x 292mm(P) x 43,5mm(H)
- Poids : 4,700 g

Alimentation
- Courant entrant : 100 - 240 Vca, 50/60 Hz, 1 A max.
- Puissance maximale : 80 Watts

Conditions de stockage et d'exploitation
- Température d'exploitation : 0 ~ 40 °C
- Humidité d'exploitation : 5 à 90 % (sans condensation)

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

Matrice des caractéristiques



Powered by Kaspersky, BlueCoat, ICSA Firewall, ICSA VPN

Content Control from BlueCoat

65-100-105002B 07/07