

Contrôle facile : Les passerelles de sécurité unifiée, un partenaire efficace !

La gamme des pare-feu ZyWALL USG propose une protection complète à votre infrastructure informatique :



1. Connexions sécurisées

Les infrastructures informatiques jouent de nos jours un rôle très important. Le développement et l'utilisation variée des technologies réseau innovantes engendrent de nombreuses nouvelles possibilités mais également quelques risques. Les entreprises doivent ainsi trouver des solutions pour établir une infrastructure appropriée qui garantit la transmission sécurisée des informations importantes sur Internet. L'infrastructure doit répondre aux besoins spécifiques tels que l'accès distant et les télétravailleurs mobiles.

2. Protection proactive

Les dangers tels que les virus, vers ou programmes nocifs peuvent s'introduire sur les réseaux d'entreprise, compromettre ceux-ci et bloquer les processus d'entreprise. En plus des pertes financières majeures ils peuvent engendrer une perte des informations confidentielles. De grandes quantités d'e-mails sont envoyées via Internet. Des quantités énormes de pourriels (spam) envahissent les réseaux d'entreprise. Si les entreprises n'utilisent pas de programmes pour détecter les e-mails spam et pour les bloquer de manière proactive, les utilisateurs doivent prendre beaucoup de temps pour vérifier leur boîte aux lettres saturée, ce qui peut engendrer une perte de productivité considérable.

3. Sécurité du réseau

De nombreux collaborateurs utilisent des applications peer to peer (P2P) et de messagerie instantanée (IM) sur les réseaux d'entreprise pour communiquer et échanger des données pendant le temps de travail. La transmission rapide de données comprenant la transmission des fichiers qui peuvent contenir des virus ne représente pas seulement un risque à la sécurité du réseau, mais elle peut également engendrer des infractions aux droits d'auteur et des conséquences juridiques.

4. Fiabilité du réseau

Pour établir une infrastructure réseau, les perturbations telles que les connexions FAI coupées, les pannes matérielles ou logicielles au niveau de l'interface ou les tunnels VPN qui ne fonctionnent pas posent de grands problèmes aux administrateurs réseau. En bref, pour établir une infrastructure réseau garantissant une haute disponibilité en service, il faut prendre en considération la tolérance de panne.

Avantages de la gamme ZyWALL USG

La gamme ZyWALL USG propose une solution de sécurité qui garantit une haute performance pour les réseaux de petite et moyenne taille à domicile ou dans les entreprises. Les pare-feu USG sont équipés d'un pare-feu Stateful Packet Inspection (SPI), antivirus, Intrusion Detection & Prevention (IDP), filtrage de contenu, anti-spam et du VPN (IPSec/SSL/L2TP) réunis dans un appareil. Ils proposent une protection complète contre les attaques intérieures et extérieures aux informations de l'entreprise et aux données des clients, à la propriété intellectuelle ainsi qu'aux données confidentielles.

1. Meilleure solution UTM de haute performance

La gamme USG utilise la technologie d'accélération matérielle dans un appareil. Grâce à la technologie performante SecuASIC et à un accélérateur matériel de cryptage, la gamme ZyWALL USG propose une très haute performance et une protection complète contre les attaques sur les réseaux d'entreprise de petite et moyenne taille. Tous les modèles ZyWALL USG disposent d'interfaces Ethernet Gigabit.

2. VPN hybride robuste (IPSec et SSL)

La gamme ZyWALL USG permet l'accès distant sécurisé aux données d'entreprise via Internet. Le VPN IPSec permet aux entreprises d'établir des connexions sécurisées aux agences, partenaires ou sites centraux. Le VPN SSL ou L2TP est conçu pour les collaborateurs mobiles et télétravailleurs, garantissant l'accès distant sécurisé au réseau d'entreprise sans devoir installer un logiciel VPN.

3. Gérer l'abus de P2P/IM

Pour améliorer la performance du réseau et augmenter la productivité, il faut gérer les applications P2P/IM de manière efficace. La gamme ZyWALL USG supporte Application Patrol qui contrôle qui a le droit d'utiliser les applications P2P et IM telles que MSN™ et BitTorrent™ et les fonctionnalités spécifiques d'une certaine application.

4. Accès à Internet sans interruption via WAN avec 3G en tant que back-up

Les pare-feu ZyWALL USG supportent de multiples ports WAN ainsi que des cartes USB 3G et PCMCIA 3G. Ainsi, ils proposent une répartition de charge « active-active » ou une configuration « active-passive » pour la fiabilité garantissant des connexions réseau de haute sécurité. Pour réduire les conséquences des pannes ponctuelles, la gamme ZyWALL USG propose une haute disponibilité matérielle garantissant ainsi la disponibilité permanente du réseau.

5. Certification ICSA pour pare-feu, IPSec et antivirus

La gamme ZyWALL USG équipée d'un pare-feu SPI certifiés ICSA, antivirus et VPN IPSec permet aux entreprises un contrôle complet de leur infrastructure réseau. Elle propose une protection complète contre les attaques sur le réseau.

6. Système de rapports détaillés

Le système de rapports intégré permet de dresser des rapports en temps réel et d'autres rapports détaillés qui informent sur les attaques des virus et d'autres dangers sur le pare-feu, la bande passante et sur les activités des utilisateurs. De plus, les administrateurs réseau peuvent utiliser le système de rapports sur page Web Vantage Report (VRPT) pour saisir des données ou superviser facilement un réseau multi-site. Les entreprises sont ainsi informées sur des activités suspectes ce qui permet de garantir une augmentation de leur productivité.

STUDERUS
network technologies

Studerus SA
Ringstrasse 1
8603 Schwerzenbach
info@studerus.ch
www.studerus.ch

ZyXEL

SECURITY

PRODUCT GUIDE 2008



Pare-feu UTM

Pare-feu avec 3G

Pare-feu mobile






Application VPN SSL

ZyXEL ZyWALL Matrice de caractéristiques

| | Sécurité des infrastructures des PME | | | | |
|---|---|---|--|---|---|
| | ZyWALL USG 100 | ZyWALL USG 200 | ZyWALL USG 300 | ZyWALL USG 1000 | ZyWALL USG 2000 |
| | Unified Security Gateways (USG) | | | | |
| |  |  |  |  |  |
| Caractéristiques | | | | | |
| Débit pare-feu | 100 Mbps | 150 Mbps | 200 Mbps | 350 Mbps | 2'000 Mbps |
| Débit VPN (AES) | 50 Mbps | 75 Mbps | 100 Mbps | 150 Mbps | 500 Mbps ^{*1} |
| Débit UTM (AV + IDP + pare-feu) | 24 Mbps | 40 Mbps | 48 Mbps | 100 Mbps | 400 Mbps ^{*2} |
| Licences d'utilisateur illimitées | ✓ | ✓ | ✓ | ✓ | ✓ |
| Sessions | 20'000 | 40'000 | 60'000 | 500'000 | 1'500'000 |
| Tunnels VPN IPSec simultanés, nombre max. | 50 | 100 | 200 | 1'000 | 2'000 |
| Utilisateurs SSL VPN, nombre min. / max. | 2 / 5 | 2 / 10 | 2 / 10 (25 ^{*3}) | 5 / 50 (250 ^{*3}) | max. 750 |
| Port physique | 5 x LAN/DMZ, 2 x WAN (tous Ethernet GB) | 4 x LAN/DMZ, 2 x WAN, 1 x OPT (tous Ethernet GB) | (7) 10/100/1000 Ethernet GB | (5) 10/100/1000 Ethernet GB | (6) 10/100/1000 Ethernet GB (2) Dual Personality Ethernet GB (SFP/RJ45) |
| Zone personnalisée | ✓ | ✓ | ✓ | ✓ | ✓ |
| Réseau | | | | | |
| Routage/NAT/mode SUA | ✓ | ✓ | ✓ | ✓ | ✓ |
| Mode pont | ✓ | ✓ | ✓ | ✓ | ✓ |
| Mode Mix (routage + pont) | ✓ | ✓ | ✓ | ✓ | ✓ |
| Tagging VLAN (802.1q) | ✓ | ✓ | ✓ | ✓ | ✓ |
| Support carte LAN sans fil | ✓ | ✓ | - | - | - |
| Support 3G | ✓ | ✓ | ✓ ^{*3} | ✓ ^{*3} | ✓ ^{*3} |
| Sécurité | | | | | |
| Pare-feu Stateful Packet Inspection | ✓ | ✓ | ✓ | ✓ | ✓ |
| VPN IPSec | ✓ | ✓ | ✓ | ✓ | ✓ |
| VPN SSL | ✓ | ✓ | ✓ | ✓ | ✓ |
| Filtrage de contenu (en option) | ✓ | ✓ | ✓ | ✓ | ✓ |
| Anti-SPAM | ✓ | ✓ | ✓ | ✓ | ✓ |
| Antivirus (en option) | ✓ | ✓ | ✓ | ✓ | ✓ |
| IDS/IDP (en option) | ✓ | ✓ | ✓ | ✓ | ✓ |
| Gestion IM/P2P | ✓ | ✓ | ✓ | ✓ | ✓ |
| Gestion de la bande passante | ✓ | ✓ | ✓ | ✓ | ✓ |
| Gestion personnalisée | ✓ | ✓ | ✓ | ✓ | ✓ |
| Haute disponibilité | | | | | |
| Haute disponibilité matérielle | A/P | A/P | A/P | A/P | A/P |
| Haute disponibilité VPN | ✓ | ✓ | ✓ | ✓ | ✓ |
| WAN multiples pour répartition de charge | ✓ | ✓ | ✓ | ✓ | ✓ |
| Fiabilité automatique, Fail-back | ✓ | ✓ | ✓ | ✓ | ✓ |
| Dial Back-up | ✓ | ✓ | ✓ | ✓ | ✓ |
| Module d'alimentation redondant | - | - | - | - | ✓ |
| Méthode d'authentification | | | | | |
| Base de données locale | ✓ | ✓ | ✓ | ✓ | ✓ |
| Rayon | ✓ | ✓ | ✓ | ✓ | ✓ |
| LDAP | ✓ | ✓ | ✓ | ✓ | ✓ |
| Microsoft AD | ✓ | ✓ | ✓ | ✓ | ✓ |
| ZyWALL OTP | ✓ | ✓ | ✓ | ✓ | ✓ |
| Gestion | | | | | |
| Interface utilisateur Web (HTTP et HTTPS) | ✓ | ✓ | ✓ | ✓ | ✓ |
| Ligne de commande | ✓ | ✓ | ✓ | ✓ | ✓ |
| Vantage CNM | ✓ | ✓ | ✓ | ✓ | ✓ |
| Vantage Report | ✓ | ✓ | ✓ | ✓ | ✓ |
| Article | 3301 | 3302 | 3303 | 3304 | 3305 |
| Prix de vente | CHF 890.- | CHF 1'240.- | CHF 2'420.- | CHF 5'340.- | dès Q3/2008 |

Note: *1: Equipé d'un module SEM-DUAL/SEM-VPN
*2: Equipé d'un module SEM-DUAL/SEM-UTM
*3: Disponible pour les futures versions du firmware.

ZyWALL Matrice de caractéristiques

| | Sécurité des bureaux à domicile et petites entreprises | | | | SSL |
|---|---|---|--|---|---|
| | ZyWALL P1 | ZyWALL 2 Plus | ZyWALL 2 WG | ZyWALL 5 | ZyWALL SSL 10 |
| | Pare-feu VPN mobile | Pare-feu VPN | Pare-feu VPN avec 3G | Pare-feu VPN | Application VPN SSL |
| |  |  |  |  |  |
| Caractéristiques | | | | | |
| Débit pare-feu | 80 Mbps | 24 Mbps | 24 Mbps | 50 Mbps | 24 Mbps |
| Débit VPN (AES) | 30 Mbps | 24 Mbps | 24 Mbps | 25 Mbps | - |
| Débit UTM (AV + IDP + pare-feu) | 5 Mbps | - | - | - | - |
| Licences d'utilisateur illimitées | ✓ | ✓ | ✓ | ✓ | - |
| Sessions | 1'500 | 3'000 | 3'000 | 4'000 | - |
| Tunnels VPN IPSec simultanés, nomb. max. | 1 | 5 | 5 | 10 | - |
| Utilisateurs VPN SSL, nombre min. / max. | - | - | - | - | 10 / 25 |
| LANS sans fil intégré | - | - | - | - | - |
| Port physique | 1 x LAN, 1 x WAN | 4 x LAN, 1 x WAN | 4 x LAN/DMZ, 1 x WAN | 4 x LAN, 1 x WAN | 4 x LAN, 1 x WAN |
| Raccordement WAN | | | | | |
| Ethernet | ✓ | ✓ | ✓ | ✓ | ✓ |
| 3G (en option) | - | - | ✓ | - | - |
| Réseau | | | | | |
| Routage/NAT/mode SUA | ✓ | ✓ | ✓ | ✓ | ✓ |
| Mode pont | ✓ | ✓ | ✓ | ✓ | - |
| Sécurité | | | | | |
| Pare-feu Stateful Packet Inspection | ✓ | ✓ | ✓ | ✓ | ✓ |
| VPN IPSec | ✓ | ✓ | ✓ | ✓ | - |
| VPN SSL | - | - | - | - | ✓ |
| Filtrage de contenu | ✓ | ✓ | ✓ | ✓ | ✓ |
| Anti-SPAM | - | - | - | ✓ | - |
| Antivirus | ✓ | - | - | - | - |
| IDS/IDP | ✓ | - | - | - | - |
| IM/P2P | ✓ | - | - | - | - |
| Gestion de la bande passante | - | ✓ | ✓ | ✓ | - |
| Gestion personnalisée | - | - | - | - | ✓ |
| Haute disponibilité | | | | | |
| Haute disponibilité VPN | ✓ | ✓ | ✓ | ✓ | - |
| WAN multiples pour répartition de charge | - | - | ✓ (3G) | - | - |
| Fiabilité automatique, Fail-back | - | ✓ | ✓ | ✓ | - |
| Dial Back-up | - | ✓ | ✓ | ✓ | - |
| Méthode d'authentification | | | | | |
| Base de données locale | ✓ | ✓ | ✓ | ✓ | ✓ |
| Rayon | ✓ | ✓ | ✓ | ✓ | ✓ |
| LDAP | - | - | - | - | ✓ |
| Microsoft AD | - | - | - | - | ✓ |
| ZyWALL OTP | ✓ | ✓ | ✓ | ✓ | ✓ |
| Gestion | | | | | |
| Interface utilisateur Web (HTTP et HTTPS) | ✓ | ✓ | ✓ | ✓ | ✓ |
| Ligne de commande | ✓ | ✓ | ✓ | ✓ | ✓ |
| Vantage CNM | ✓ | ✓ | ✓ | ✓ | - |
| Vantage Report | ✓ | ✓ | ✓ | ✓ | - |
| Article | 2807 | 2801 | 2808 | 2806 | 2855 |
| Prix de vente | CHF 290.- | CHF 340.- | CHF 460.- | CHF 780.- | CHF 560.- |