

ZyXEL

Combattez les **malwares** !



Filtrage de contenu
Application Guide

2011

- Une offre complète
- Des technologies de pointe
- Un fournisseur unique pour une solution globale



Introduction

Contrôler l'accès à Internet et bloquer les attaques en ligne

L'évolution d'Internet rend le contrôle des activités sur le web et l'allocation de bande passante de plus en plus difficile. De plus, les nouvelles sources de menaces en ligne demandent une protection renforcée. Le filtrage de contenu des ZyWALL USG (boîtiers de sécurité unifiée) basé sur les technologies Blue Coat empêche les téléchargements de malwares, protège les utilisateurs contre les menaces en ligne et permet de mettre en place une sécurité adaptée aux besoins de l'entreprise assurant une productivité optimale des employés. Le service de filtrage de contenu du pare-feu ZyWALL USG est régulièrement mis à jour via WebPulse (service communautaire Blue Coat), assurant ainsi une sécurité à jour contre les derniers malwares.

Le service WebPulse capitalise sur le potentiel du cloud computing pour analyser le plus grand nombre de sites web. De plus, dès qu'un nouveau malware est découvert via WebPulse, l'information est aussitôt partagée au sein de la communauté. Le filtrage de contenu ZyWALL est mis à jour à travers le cloud (nuage), garantissant ainsi une catégorisation pertinente des sites et en temps réel. WebPulse recherche les codes injectés sur les sites web les plus visités (en effectuant des inspections DLA, Dynamic Link Analysis) et contrôle les résultats des moteurs de recherche pour détecter les sites pièges – tout deux fonctionnant grâce à des liens dynamiques. En couplant les technologies anti-malware et la catégorisation des URL, le service de filtrage de contenu des ZyWALL USG utilise les technologies de nouvelle génération pour protéger les utilisateurs grâce à un système de défense communautaire.

Table des matières

Introduction	2
Des menaces qui évoluent	3
Combattez les malwares !	5
Catégorisation des URL dans le filtrage de contenu	6

Des menaces qui évoluent

La propagation des malwares

Internet est aujourd'hui le vecteur privilégié pour propager les menaces contre les réseaux et autres logiciels malveillants. En effet, les malwares se cachent de préférence directement dans les contenus des pages web, sous la forme de cookies, d'add-on et de rootkits. Ils deviennent, de ce fait, très difficiles à trouver. Les réseaux sont confrontés aujourd'hui à de nombreux dangers, incluant :

- **Volume de codes malveillants sans précédent** : le volume de logiciels malveillants de toute forme a quasiment triplé depuis 2009
- **Menaces en ligne** : en raison de la popularité croissante du Web 2.0, plus de 40 % des attaques visent le navigateur.
- **Attaque via les réseaux sociaux** : environ 40 % des utilisateurs de réseaux sociaux ont déjà été victimes d'une attaque.
- **Attaques ciblées** : les attaques web peuvent viser une région, une entreprise ou un service, sans nécessairement être lancées immédiatement.

Les trois risques principaux pour les entreprises

La diversité des malwares est devenu un problème sérieux qui pèse sur les réseaux informatiques des entreprises. Si celles-ci ne se dotent pas de moyens de défense efficaces, elles subiront de plein fouet l'impact des malwares dont voici les risques :

- **Risques de sécurité réels** : lorsque le personnel consulte des pages web potentiellement dangereuses, qui installent et exécutent des logiciels malveillants de façon automatique, le risque de corruption de la sécurité du réseau est réel.
- **Coûts informatiques** : l'analyse des ordinateurs, l'élimination du malware et la réinstallation des programmes ou la récupération des fichiers représentent un coût élevé pour une entreprise.
- **Divulgence et revente de données sensibles** : l'objectif des malwares est souvent d'accéder à des données sensibles par le biais d'un poste infecté. Ces données peuvent ensuite être revendues, notamment à la concurrence.

Pourquoi votre solution de sécurité actuelle ne suffit plus ?

Les codes malveillants sont omniprésents. Les systèmes de sécurité basés sur les signatures doivent relever deux défis majeurs pour pouvoir répondre à un très grand nombre de menaces qui changent chaque jour :

- **1) Véritable explosion du volume de malwares** : les solutions de sécurité qui s'appuient uniquement sur des bases de données de signatures sont des solutions complètes, mais dont la mise à jour est constante et laborieuse : en effet, pour chaque menace détectée, le prestataire doit l'isoler, développer une signature, et la diffuser auprès des millions de systèmes informatiques qu'il doit protéger. Ce processus peut prendre de quelques heures à plusieurs jours, en fonction de la complexité de la menace.
- **2) La surenchère des menaces** : dans la masse de liens dynamiques reçus chaque jour, tout élément peut diriger vers un contenu infecté, même lorsqu'il provient de sites de confiance. Le temps que les outils de sécurité identifient l'attaque, les systèmes sont souvent déjà infectés.



Quelle stratégie adopter ?

Une solution de sécurité efficace est caractérisée par une stratégie de défense multi-niveaux qui s'attaque aux dangers actuels non reconnus par les outils de sécurité classiques. Les deux facteurs suivants sont décisifs pour le succès d'une solution de sécurité en entreprise :

1 S'appuyer sur une communauté collaborative

Une vaste communauté collaborative au sein de laquelle la découverte d'un nouveau malware est aussitôt partagée en temps réel par tous les membres.

2 Se baser sur un service « cloud computing »

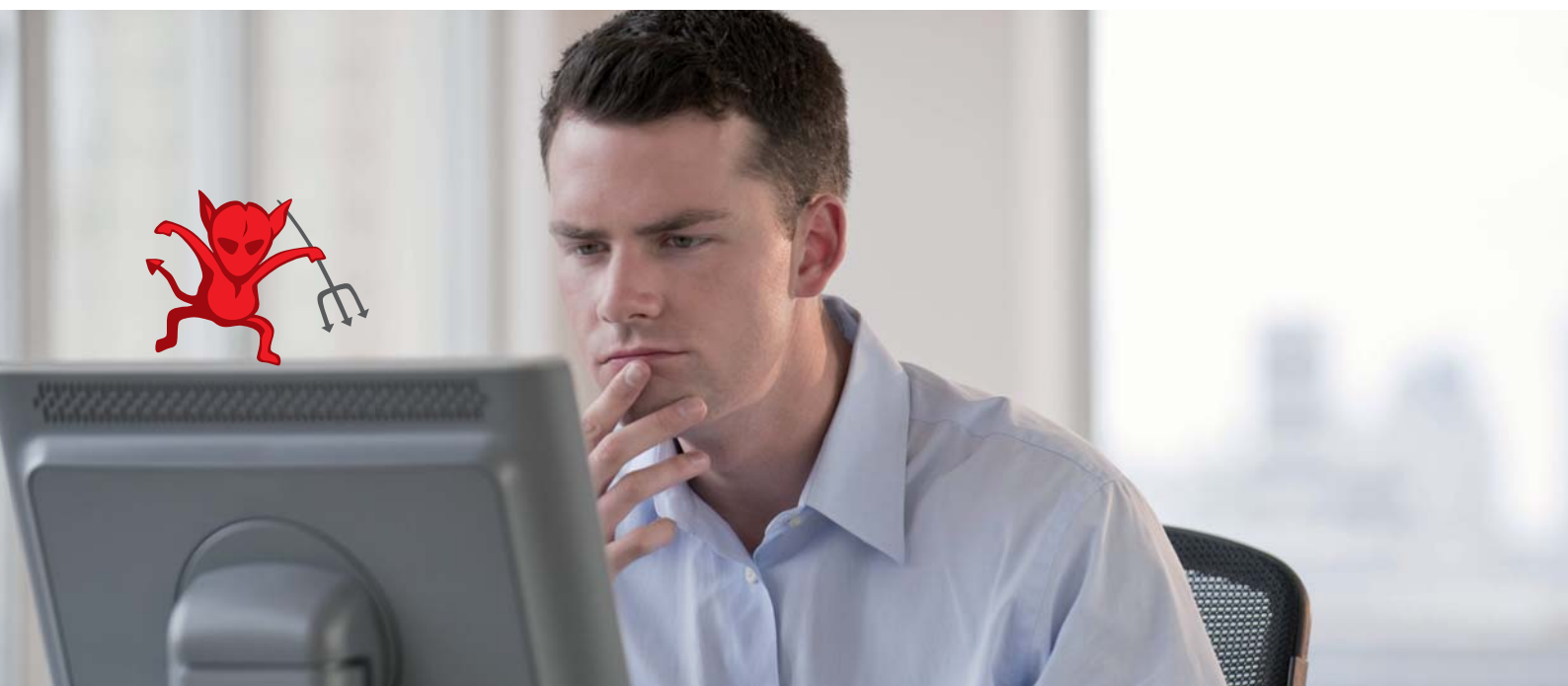
Les services basés sur le cloud computing complètent les passerelles de sécurité et les bases de données de signatures, en créant une architecture de défense approfondie.

Grâce à ses deux atouts, les systèmes de sécurité basés sur le cloud permettront de se protéger contre les menaces dernières générations, toujours plus rapides, plus nombreuses, et

en constante évolution. En effet, ils se basent sur une communauté qui découvre perpétuellement de nouveaux malwares, bloque les contenus Internet inconnus, les analysant en temps réel, en mettant immédiatement à jour les bases de signatures.

■ **Identification des nouvelles menaces d'Internet en temps réel** : les experts de la sécurité en ligne et les moteurs de détection de menaces proposent une analyse détaillée et fiable des contenus web, URLs, adresses IP et protocoles via le cloud et en temps réel.

■ **Une approche communautaire pour un maximum d'efficacité** : les solutions de sécurité basées sur le cloud sont conçues pour empêcher les incidents, et analyser, catégoriser et bloquer les malwares avant qu'ils ne se propagent dans les réseaux et infectent les systèmes.



Combattez les malwares !

1 Détection et prévention

Le filtrage de contenu ZyXEL analyse et classe quotidiennement plus de 6 milliards de pages web pour le compte de plus de 70 millions d'utilisateurs à travers le monde, dans les plus grandes entreprises et chez les fournisseurs d'accès :

- WebPulse compte à ce jour 8 centres d'analyse via le cloud, traitant plus d'un milliard de requêtes web par semaine.
- Les nouveaux liens ou contenus Internet détectés par les passerelles web ou les clients ayant accès à distance sont envoyés en temps réel sur le cloud WebPulse pour une inspection DLA, où les mises à jour du BlueCoat WebFilter assurent une protection immédiate.
- Le filtrage de contenu ZyXEL bloque les malwares, menaces, contrefaçons de mise à jour de logiciels et d'offres d'antivirus, ainsi que les attaques d'hameçonnage (phishing).
- Les sites sont bloqués via des inspections DLA, ce qui permet aux utilisateurs de continuer à naviguer sur Internet en évitant les blocages intempestifs.
- WebPulse permet sur le Web 2.0 le filtrage des pages à contenu multisource, comme par exemple les forums, en bloquant les contenus dynamiques en fonction des règles de sécurité.
- WebPulse couvre plus de 50 langues et utilise des algorithmes propriétaires pour l'analyse automatique des contenus.
- Le filtrage de contenu des ZyWALL USG intègre des informations malware de Google ainsi que des classifications des parties tiers sur les menaces en ligne.

2 Précision et pertinence

Les ZyWALL USG de ZyXEL proposent un filtrage de contenu basé non pas sur une analyse automatique des sites, mais sur l'analyse des sites par une communauté large et diversifiée d'utilisateurs :

- Le filtrage de contenu des ZyWALL USG s'approprie rapidement les habitudes des nouveaux utilisateurs, leur proposant ainsi un classement pertinent des nouveaux sites en temps réel

- Le filtrage de contenu des USG effectue la classification des sites de confiance et permet aux entreprises d'opter soit pour une analyse des menaces de manière intégrée, soit pour le blocage de tout téléchargement, comme les fichiers d'installation de programme ou les fichiers exécutables provenant des sites non référencés « de confiance ».

3 Efficacité et sécurité

Grâce aux technologies WebPulse de Blue Coat, le filtrage de contenu ZyXEL propose une protection Web 2.0, une classification des contenus web de la communauté ainsi que des fonctionnalités préventives sur le cloud ou sur la passerelle garantissant un très haut niveau de protection :

- Les téléchargements et les patch deviennent obsolètes, puisque la passerelle web et les clients distants communiquent avec le cloud et reçoivent des mises à jour automatiques en temps réel.
- La technologie Web 2.0 est protégée via une combinaison de filtrage URL et de fonction de Détection et prévention d'intrusion (IDP). L'approche cloud communautaire permet de détecter le malware, les fausses mises à jour de logiciels, les scamwares et les attaques d'hameçonnage.

4 Visibilité et reporting

Le filtrage de contenu des ZyWALL USG couplé au logiciel de reporting Vantage Report garantit une surveillance complète et professionnelle des passerelles et assure le respect des règles de filtrage :

- Le tableau de bord donne une vue d'ensemble de l'état actuel des menaces potentielles. Les administrateurs reçoivent un compte rendu journalier généré de manière automatique.
- Le logiciel Vantage Report permet de gérer de manière centralisée tous les ZyWALL USG installés sur différents sites. Les fonctions de reporting facilitent le contrôle de l'utilisation qui est faite d'Internet par les employés et aident les administrateurs à détecter rapidement les menaces sur le réseau. De plus, les fonctions d'archivage et de recherche des fichiers logs donnent rapidement les informations qui vont permettre de faire appliquer une politique de sécurité au sein de l'entreprise.



Catégorisation des URL dans le filtrage de contenu USG ZyWALL par Bluecoat

La catégorisation des URL

La banque de données du filtrage de contenu pour ZyWALL USG inclut des millions de classifications web, correspondant à des milliards de pages web. La banque de données couvre plus de 50 langues et 78 catégories de sites.

Security Threat (unsafe)		
<input checked="" type="checkbox"/> Phishing	<input checked="" type="checkbox"/> Spyware/Malware Sources	<input checked="" type="checkbox"/> Spyware Effects/Privacy Concerns
<input checked="" type="checkbox"/> Proxy Avoidance		
Managed Categories		
Adult Related		
<input checked="" type="checkbox"/> Adult/Mature Content	<input type="checkbox"/> Alternative Sexuality/Lifestyles	<input type="checkbox"/> Extreme
<input type="checkbox"/> Intimate Apparel/Swimsuit	<input checked="" type="checkbox"/> Nudity	<input checked="" type="checkbox"/> Pornography
<input type="checkbox"/> Open/Mixed Content	<input type="checkbox"/> Sex Education	
Liability Concerns		
<input checked="" type="checkbox"/> Illegal Drugs	<input type="checkbox"/> Illegal/Questionable	<input checked="" type="checkbox"/> Gambling
<input type="checkbox"/> Violence/Hate/Racism	<input type="checkbox"/> Weapons	
Security Concerns		
<input checked="" type="checkbox"/> Hacking	<input checked="" type="checkbox"/> Pay to Surf	<input type="checkbox"/> Placeholders
<input checked="" type="checkbox"/> Potentially Unwanted Software	<input type="checkbox"/> Remote Access Tools	<input type="checkbox"/> Suspicious
File Transfer		
<input type="checkbox"/> Online Storage	<input type="checkbox"/> Peer-to-Peer	<input type="checkbox"/> Software Downloads
Society/Government		
<input type="checkbox"/> Alternative Spirituality/Occult	<input type="checkbox"/> Cultural/Charitable Organizations	<input type="checkbox"/> Government/Legal
<input type="checkbox"/> LGBT	<input type="checkbox"/> Military	<input type="checkbox"/> Political/Activist Groups
<input type="checkbox"/> Religion	<input type="checkbox"/> Society/Lifestyle	
Social Interaction		
<input type="checkbox"/> Blogs Personal Pages	<input type="checkbox"/> Greeting Cards	<input type="checkbox"/> Personals/Dating
<input type="checkbox"/> Social Networking		
Multimedia		
<input type="checkbox"/> Audio/Video Clips	<input type="checkbox"/> Media Sharing	<input type="checkbox"/> Radio/Audio Streams
<input type="checkbox"/> TV/Video Streams		
Communication		
<input type="checkbox"/> Chat/Instant Messaging	<input type="checkbox"/> Email	<input type="checkbox"/> Internet Telephony
<input type="checkbox"/> Online Meetings	<input type="checkbox"/> Newsgroups/Forums	
Health Related		
<input type="checkbox"/> Abortion	<input type="checkbox"/> Alcohol	<input type="checkbox"/> Health
<input type="checkbox"/> Restaurants/Dining/Food	<input type="checkbox"/> Tobacco	
Leisure		
<input type="checkbox"/> Arts/Culture	<input type="checkbox"/> Entertainment	<input type="checkbox"/> For Kids
<input type="checkbox"/> Games	<input type="checkbox"/> Humor/Jokes	<input type="checkbox"/> Sports/Recreation
Commerce		
<input type="checkbox"/> Brokerage/Trading	<input type="checkbox"/> Business/Economy	<input type="checkbox"/> Financial Services
<input type="checkbox"/> Job Search/Careers	<input type="checkbox"/> Real Estate	<input type="checkbox"/> Auctions
<input type="checkbox"/> Shopping	<input type="checkbox"/> Travel	<input type="checkbox"/> Vehicles
<input type="checkbox"/> Web Advertisements		
Technology		
<input type="checkbox"/> Computers/Internet	<input type="checkbox"/> Content Servers	<input type="checkbox"/> Non Viewable
<input type="checkbox"/> Web Hosting	<input type="checkbox"/> Web Applications	
Information Related		
<input type="checkbox"/> Education	<input type="checkbox"/> News/Media	<input type="checkbox"/> Reference
<input type="checkbox"/> Search Engines/Portals	<input type="checkbox"/> Translation	

Blue Coat WebPulse : une défense sur le cloud

Les malwares se développent continuellement et exigent des entreprises une stratégie de défense flexible permettant de faire face à ces nouvelles menaces en ligne. Les requêtes web d'une communauté de plus de 70 millions d'utilisateurs à travers le monde, analysées sur le cloud par WebPulse, assurent un très haut niveau de protection en temps réel. WebPulse prend en charge plus de 50 langues et dispose de puissants mécanismes de recherche (des moteurs de détection « Multiple Threat ») pour détecter les dangers sur le web. Au total, WebPulse assure la classification de plus de six milliards de requêtes web par jour.

Le service WebPulse fait partie intégrante de la solution de filtrage de contenu ZyWALL USG, offrant une défense rapide et efficace du Web 2.0. grâce à l'analyse de scripts, au scan anti-malware et anti-virus mais aussi grâce au mécanisme « sandbox » et à la simulation de navigateurs et bien d'autres technologies de sécurité au service de ses nombreux utilisateurs:

- Analyse dynamique des requêtes URL et partage immédiat des résultats avec la communauté sur le cloud
- Plus de 16 outils d'analyse pour une protection efficace contre les nouveaux dangers ou les menaces inconnues sur le web
- Les derniers progrès dans le domaine de la sécurité web sont tout de suite partagés avec toute la communauté, sans téléchargements de logiciels ou mises à jour

A propos des boîtiers de sécurité ZyWALL USG

Le concept de sécurité supporté par les pare-feux ZyXEL couvre tous les domaines des communications en entreprise. Les pare-feux ne laissent entrer que les contenus désirés sur le réseau, la fonction anti-spam se charge du scan des e-mails, le filtrage de contenu bloque l'accès aux sites non désirés ou dangereux. De plus, le service anti-virus empêche les virus, chevaux de Troie et spywares d'entrer sur le réseau, tandis que l'IDP (Détection et prévention d'intrusion) détecte et élimine les malwares selon des schémas d'activité précis. Le support VPN, garantit une connexion sécurisée à distance via des tunnels IPSec, SSL ou L2TP. Le trafic de données peut être contrôlé via des règles de pare-feu, les contenus étant protégés par des fonctionnalités anti-virus et IDP. L'Application Patrol localise et empêche le trafic non autorisé.

Toutes ces fonctionnalités, réunies au sein d'un même boîtier, offrent une protection contre les hackers. ZyXEL propose des solutions qui ne sont pas seulement efficaces mais également conviviales, à un prix attractif. Toutes les mises à jour sont effectuées de manière automatique et les mises à jour de firmware sont disponibles gratuitement et sans limitation dans le temps.





Corporate Headquarters

ZyXEL Communications Corp.

Tel: +886-3-578-3942
Fax: +886-3-578-2439
Email: sales@zyxel.com.tw
<http://www.zyxel.com>

■ Europe

ZyXEL Belarus

Tel: +375 17 334 6099
Fax: +375 17 334 5899
Email: sales@zyxel.by
<http://www.zyxel.by>

ZyXEL Benelux

Tel: +31 23 5553689
Fax: +31 23 5578492
Email: sales@zyxel.nl
<http://www.zyxel.nl>
<http://www.zyxel.be>

ZyXEL Czech

Tel: +420 241 091 350
Fax: +420 241 091 359
Email: info@cz.zyxel.com
<http://www.zyxel.cz>

ZyXEL Denmark A/S

Tel: +45 39 55 07 00
Fax: +45 39 55 07 07
Email: sales@zyxel.dk
<http://www.zyxel.dk>

ZyXEL Finland

Tel: +358-9-4780 8400
Email: myynti@zyxel.fi
<http://www.zyxel.fi>

ZyXEL France

Tel: +33 (0)4 72 52 97 97
Fax: +33 (0)4 72 52 19 20
Email: info@zyxel.fr
<http://www.zyxel.fr>

ZyXEL Germany GmbH

Tel: +49 (0) 2405-6909 0
Fax: +49 (0) 2405-6909 99
Email: sales@zyxel.de
<http://www.zyxel.de>

ZyXEL Hungary & SEE

Tel: +36-1-336-1640
Fax: +36-1-325-9100
Email: info@zyxel.hu
<http://www.zyxel.hu>

ZyXEL Italy

Tel: 800 99 26 04
Fax: +39 011 274 7647
Email: sales@zyxel.it
<http://www.zyxel.it>

ZyXEL Norway

Tel: +47 22 80 61 80
Fax: +47 22 80 61 81
Email: salg@zyxel.no
<http://www.zyxel.no>

ZyXEL Poland

Tel: +48 (22) 333 8250
Fax: +48 (22) 333 8251
Email: info@pl.zyxel.com
<http://www.zyxel.pl>

ZyXEL Russia

Tel: +7 (495) 542-8920
Fax: +7 (495) 542-8925
Email: info@zyxel.ru
<http://www.zyxel.ru>

ZyXEL Slovakia

Tel: +421 243 193 989
Fax: +421 243 193 990
Email: info@sk.zyxel.com
<http://www.zyxel.sk>

ZyXEL Spain

Tel: +34 902 195 420
Fax: +34 913 005 345
Email: sales@zyxel.es
<http://www.zyxel.es>

ZyXEL Sweden A/S

Tel: +46 8 5776060
Fax: +46 8 5776061
Email: sales@zyxel.se
<http://www.zyxel.se>

ZyXEL Switzerland

Tel: +41 (0)44 806 51 00
Fax: +41 (0)44 806 52 00
Email: info@zyxel.ch
<http://www.zyxel.ch>

ZyXEL Turkey A.S.

Tel: +90 212 314 18 00
Fax: +90 212 220 25 26
Email: bilgi@zyxel.com.tr
<http://www.zyxel.com.tr>

ZyXEL UK Ltd.

Tel: +44 (0) 118 9121 700
Fax: +44 (0) 118 9797 277
Email: sales@zyxel.co.uk
<http://www.zyxel.co.uk>

ZyXEL Ukraine

Tel: +380 44 494 49 31
Fax: +380 44 494 49 32
Email: sales@ua.zyxel.com
<http://www.ua.zyxel.com>

■ Asia

ZyXEL China (Shanghai) China Headquarters

Tel: +86-021-61199055
Fax: +86-021-52069033
Email: sales@zyxel.cn
<http://www.zyxel.cn>

ZyXEL China (Beijing)

Tel: +86-010-62602249
Email: sales@zyxel.cn
<http://www.zyxel.cn>

ZyXEL China (Tianjin)

Tel: +86-022-87890440
Fax: +86-022-87892304
Email: sales@zyxel.cn
<http://www.zyxel.cn>

ZyXEL India

Tel: +91-11-4760-8800
Fax: +91-11-4052-3393
Email: info@zyxel.in
<http://www.zyxel.in>

ZyXEL Kazakhstan

Tel: +7-727-2-590-699
Fax: +7-727-2-590-689
Email: info@zyxel.kz
<http://www.zyxel.kz>

ZyXEL Malaysia

Tel: +603-7960-0088
Fax: +603-7960-8802
Email: info@zyxel.com.my
<http://www.zyxel.com.my>

ZyXEL Pakistan

Tel: +92 213 4310194-5
Fax: +92 213 4310196
Email: info@zyxel.com.pk
<http://www.zyxel.com.pk>

ZyXEL Singapore

Tel: +65-6899-6678
Fax: +65-6899-8887
Email: sales@zyxel.com.sg
<http://www.zyxel.com.sg>

ZyXEL Taiwan (Taipei)

Tel: +886-2-2739-9889
Fax: +886-2-2735-3220
Email: sales_tw@zyxel.com.tw
<http://www.zyxel.com.tw>

ZyXEL Thailand

Tel: +66-(0)-2831-5315
Fax: +66-(0)-2831-5395
Email: info@zyxel.co.th
<http://www.zyxel.co.th>

■ The Americas

ZyXEL Costa Rica

Tel: +506-22017878
Fax: +506-22015078
Email: sales@zyxel.co.cr
<http://www.zyxel.co.cr>

ZyXEL USA

North America Headquarters
Tel: +1-714-632-0882
Fax: +1-714-632-0858
Email: sales@zyxel.com
<http://us.zyxel.com>

Plus d'informations sur : www.zyxel.fr

Copyright © 2011 ZyXEL Communications Corp. Tous droits réservés. ZyXEL et le logo ZyXEL sont des marques déposées de ZyXEL Communications Corp. Toutes les autres marques, tous les autres noms de produits sont propriétés de leurs propriétaires respectifs. Toutes les données techniques peuvent être modifiées sans préavis.