ZyXEL

Unified UTM Power
Get Full Control over Your Network with the New ZyXEL USG Series

USG110 UNIFIED SECURITY GATEWAY

USG210 UNIFIED SECURITY GATEWAY

USG1100 UNIFIED SECURITY GATEWAY

USG1900 UNIFIED SECURITY GATEWAY

USG40W UNIFIED SECURITY GATEWAY

USG40 UNIFIED SECURITY GATEWAY

USG60 UNIFIED SECURITY GATEWAY

USG60W UNIFIED SECURITY GATEWAY

Application Guide

Next Generation USG Series

ZyXEL

USG40W
UNIFIED SECURITY GATEWAY

PWR   SYS   USB   WLAN   WAN
                                  P1   LAN/DMZ
                              10/100/1000   P2   P3   P4   OPT
                                                              10/100/1000   P5

KEL

G40
RITY GATEWAY

PWR   SYS   USB   WAN
                               P1   LAN/DMZ
                           10/100/1000   P2   P3   P4   OPT
                                                           10/100/1000   P5

Table of Contents

ZyXEL Unified Security Gateway Range — Seriously Tough Integrated Security for the SMB

Security threats to the SMB— Why traditional firewalls can't keep you covered

With business success more dependent on 24/7 connectivity and data availability than ever, the cost of a data breach to your business has never been greater. In fact, the sad truth is, that many SMB's never recover from the financial losses and reputational damage caused by a single successful attack, or careless employee leak.

Unfortunately, it is an unavoidable reality that new threats to the SMB are emerging daily. Malicious apps, denial of service attacks, spyware and malware have all become part of the landscape of business today. The recent revelation of the SSL Heartbleed bug is just one example of how vulnerable our business systems can be to data theft and attack.

In addition to malicious attacks, unproductive internet use, such as social networking, gaming and even gambling, can have a hugely detrimental impact on staff productivity, and can open the door for network attacks.
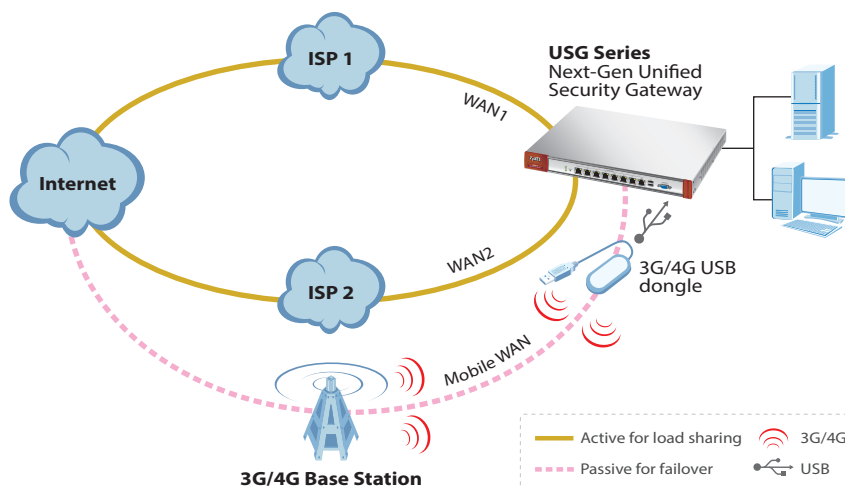
Traditional firewalls were never designed to combat these threats. This means that a new approach, one that is application and content aware, is the only way to safeguard modern businesses from the ever increasing array of security challenges that originate from within the business as well as outside.

That is why the ZyXEL USG series is leading the way in Unified Threat Management, and is already protecting the data assets, operational continuity and the reputation of ZyXEL customers all over the world. This guide will help you to advise your customers in when they encounter security concerns and to convince them by offering tailor-made security solutions. It presents a great variety of business scenarios, providing you with detailed descriptions and a diagram for each scenario. The ZyXEL complete security portfolio is also presented for offering best solution which meats unique needs of your customers.

How to Ensure Non-stop Connectivity to the Internet?

USG Series
Next-Gen Unified
Security Gateway

ISP 1

Internet

ISP 2

WAN1

WAN2

Mobile WAN

3G/4G USB dongle

3G/4G Base Station

— Active for load sharing   3G/4G
- - - Passive for failover   USB

Solution

A Wide Area Network (WAN) covering a broad area connects a private network, such as a Local Area Network (LAN), to another or the Internet. That way, computers on one location can communicate with computers elsewhere. The ZyXEL USG Series provides non-stop Internet uptime with multi-WAN and mobile broadband support. Multi-WAN works with two or more Ethernet WAN connections for active-active WAN load balancing or active-passive failover. Comprehensive mobile broadband USB modems are also supported for WAN backup.

Load balancing will be further described in Scenario 2. Here we will demonstrate the scenario for unlimited Internet access as the primary WAN, and perform mobile broadband backups through USB; that is, the USG normally uses the primary WAN interface for Internet access and will switch to the mobile broadband interface if the primary WAN connection fails.

Performance Features

- Multiple WAN ports for load sharing and failover
- Non-stop Internet access with multiple WAN and mobile broadband backups
- Supports to 2 modes:
  - active-active for load sharing
  - active-passive for failover
- Supports more 3G/4G USB modems for WAN backup

Application Benefits

- Keep your business connected even when the Internet goes down
- Flexible mobile broadband backup as a WAN alternative to increase availability
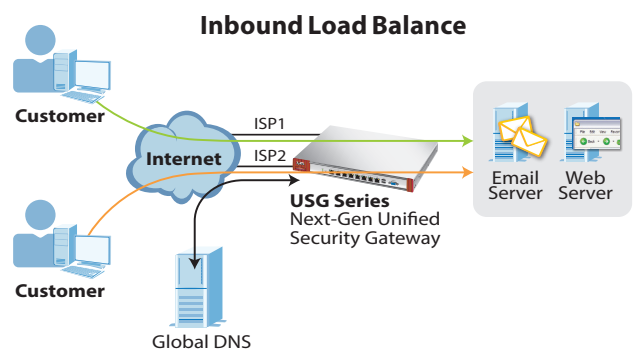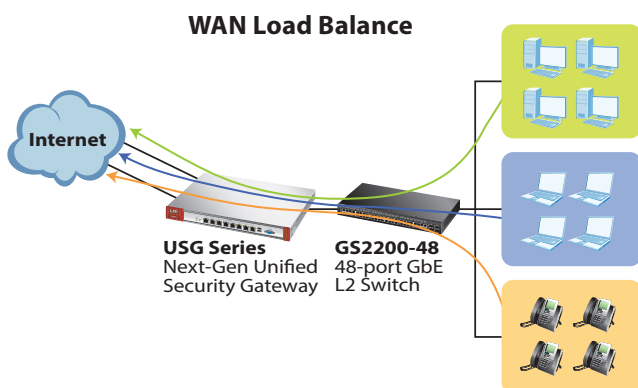- Smooth, highly reliable network connectivity

How to Get Internet Connections Utilized Effectively?

Solution

As a business network gateway, the USG Series usually has more than one WAN connection to share the network traffics. Without WAN load balancing, a single WAN connection may get too congested so that the Internet traffic would become slow or even lost. Since the outbound traffic on the USG is distributed to multiple Internet connections, traffics can get passed through the USG smoothly to improve service quality and to ensure the efficiency of Internet connection. The USG can even re-route different traffic types such as VoIP, HTTP and others to different WAN connections on demand.

To ensure non-stop application services to customers, the USG offers inbound load balancing to respond to DNS query messages with the least IP address of the loaded interface; the DNS query senders will then transmit packets to that interface instead of the ones having heavy loads. After the DNS query, the USG can reply via another WAN IP to the client according to networking status, so customers can visit the servers behind USG smoothly. If one WAN port is congested, USG will automatically assign another WAN connection to help customers to access the servers successfully.

WAN Load Balance

Internet

USG Series
Next-Gen Unified
Security Gateway

GS2200-48
48-port GbE
L2 Switch

Inbound Load Balance

Customer

Internet

ISP1
ISP2

USG Series
Next-Gen Unified
Security Gateway

Email Web
Server Server

Customer

Global DNS

Performance Features
- Flexible ways to implement WAN load balancing on demand
- WAN load balancing algorithm:
  - WRR — Weighted Round Robin
  - LLF — Least Load First
  - Spill-over

Application Benefits
- Increased overall network throughput and resilience
- Reduced need for costly bandwidth upgrades
- Non-stop services that improve customer experience
- Total control and secure global application delivery
- DNS inbound load balance

How to Protect Business from Spams?
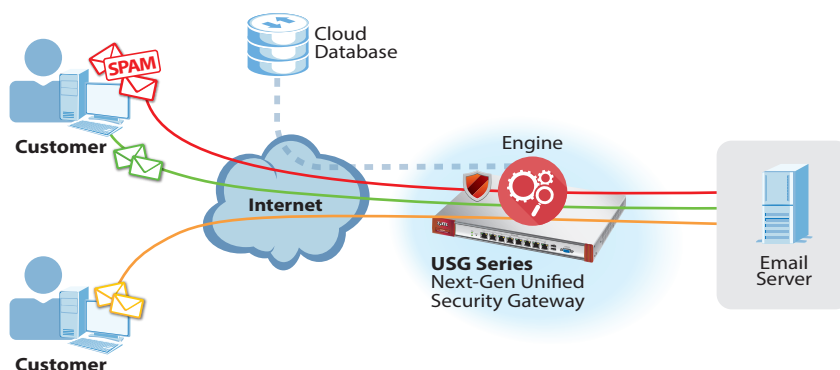
Solution

With fraudulent, inappropriate and offensive emails being delivered in vast quantities to adults, children and businesses every day, spam protection is an essential component of your network security strategy. Spam wastes time and resource of network users, and they're dangerous too. To address this, the USG Series provides Anti-Spam features to keep spam off your network.

With a cloud-based IP reputation system, ZyXEL anti-spam can deliver accurate, zero-hour spam outbreak protection by analyzing up-to-the-minute sender reputation data from highly diverse traffic sources. ZyXEL's Anti-Spam service not only filters out spams and malware, its smart report function also tags e-mail messages to remind end-users that the particular mails could be spams or have been infected; in addition, administrators can also set custom rules to filter out emails in question.
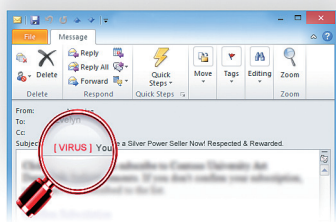
Performance Features

- Transparent mail interception via SMTP and POP3 protocols
- Configurable POP3 and SMTP ports
- Sender-based IP reputation filter
- Recurrent Pattern Detection (RPD) technology
- Zero-hour virus outbreak protection
- X-Header support
- Blacklist and whitelist support
- Supports DNSBL checking
- Spam tag support
- Statistics report

Application Benefits

- Reducing waste of necessary system resources
- Saving bandwidth and enhancing performance
- Increasing information security
- Built-in compliance capabilities
- Outstanding capability on threats anticipation

How to Protect Employee from Unsafe Web Sites with Potential Malware Attacks?
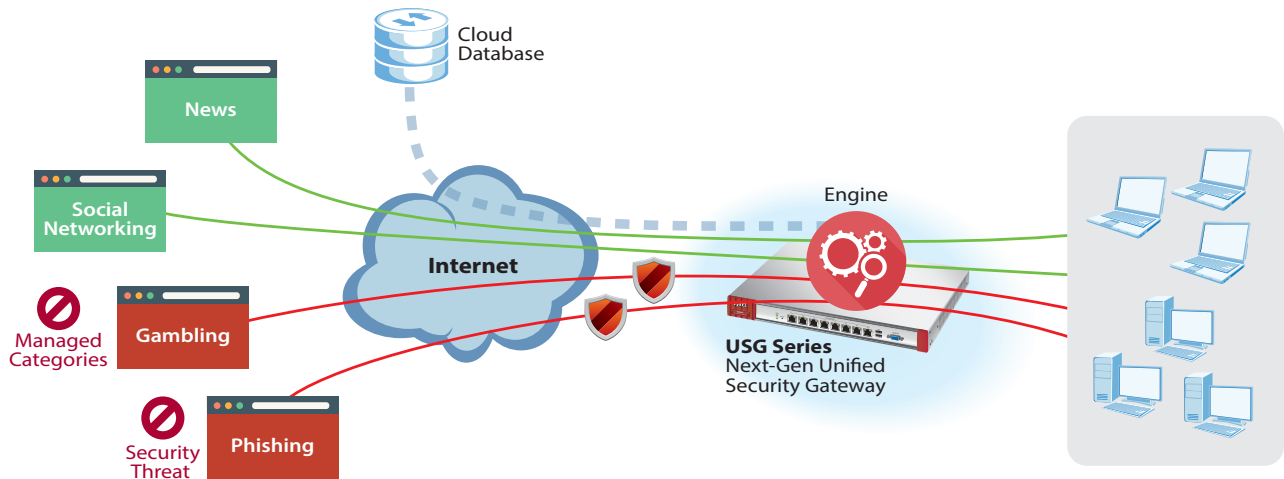
Solution

The content filter built into the USG Series is the best solution that collectively addresses the speed, variety and ever-changing nature of today's threats, thanks to its large diverse community, constant threat discovery, blocking of unknown Web contents, real-time analysis and immediate signature updates.

- **Cloud detection for real time protection**: ZyXEL's content filtering function employs the pattern detection scan system to drive our optimized filtering technology for improved performance and accuracy. Accurate category detection supports embedded URLs to ensure precise filtering, and it detects shortened URLs if the URLs have been relayed. We provide an outstanding filtering engine as well as a robust cloud-based service structure to ensure zero-delay category detection.

- **High-accuracy coverage**: the cloud-based community security is designed for incident prevention and threat analyzing, rating and blocking before they can penetrate networks and infect systems from global coverage with near zero latency ZyXEL content filtering helps screen access to websites that are not business related or malicious. With a massive, cloud-based database of over 140 billion URLs that are continuously analyzed and tracked, ZyXEL provides highly accurate, broad and instant protection against malicious Web content.
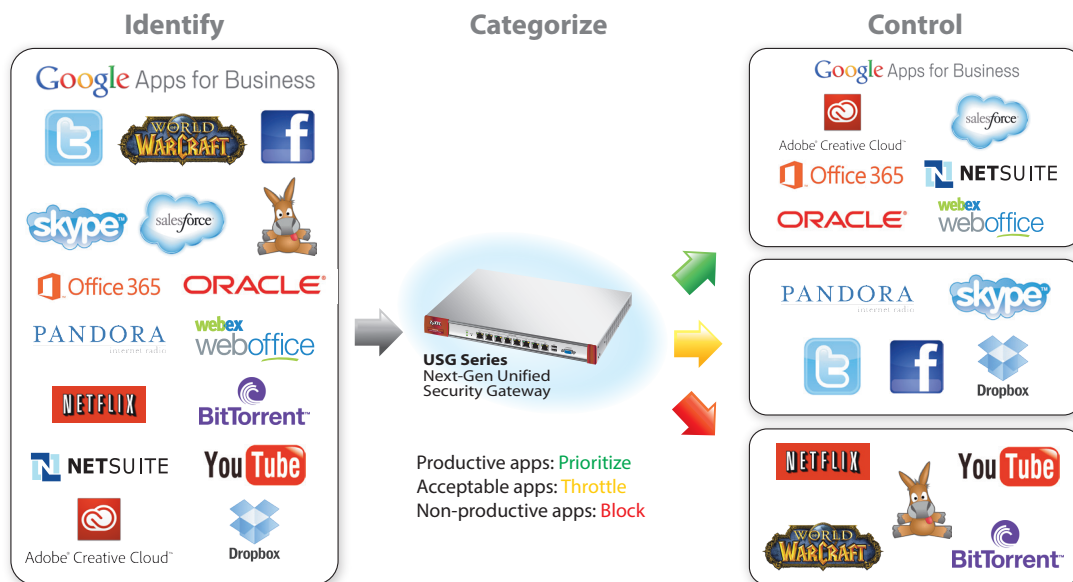
Performance Features

- Social media filtering
- Malicious Website filtering
- URL blocking and keyword blocking
- Blacklist and whitelist support
- Blocks java applets, cookies and ActiveX
- Dynamic, cloud-based URL filtering database
- Unlimited user license support
- Customizable warning messages and redirection URL
- SSL (HTTPS) inspection support
- Block/warn/log behaviors for different managed rules

Application Benefits

- **Massive scalability protection** — enabling real-time protection from emerging Web threats including malware and phishing from global coverage
- **Increased employee productivity** — categorizing and blocking amusements sites (e.g online shopping and social networking) to maximize employee productivity
- **Bandwidth regulation** — identifying sites that consume a significant amount of bandwidth (e.g. media streaming and download site)

How to Ensure Employee Productivity?

Identify

Categorize

USG Series
Next-Gen Unified
Security Gateway

Productive apps: Prioritize
Acceptable apps: Throttle
Non-productive apps: Block

Control

Solution

Businesses lose productivity when employees waste time chatting, download illegal files and visiting non-business related sites such as Facebook or Twitter. The wasted bandwidth not only produces no benefit to the company, but critical work-related Internet activities of themselves and even the colleagues will also be affected.

With the "Application Intelligence" function on the USG Series, you have granular control of IM, P2P, gaming and social networking applications down to the individual users. You can allow apps necessary to the business but restrict them to a specific group of users, a defined prioritize time period and bandwidth management. (IM/P2P requires an IDP service license).

Performance Features

- Granular control over the most important applications
- Identifies and controls over 3,000 applications and behaviors
- Supports over 15 application categories
- Application bandwidth management
- Supports user authentication
- Real-time statistics and reports
- SSL (HTTPS) inspection support

Application Benefits

- Save money and increase productivity
- Granular, precise and control over each employee/department's access privilege
- Less danger from Internet abuse
- Limit policy for Social Media sites such as posting or chatting to maximize employee productivity
- Flexibility control over bandwidth and use policy for download application and media streaming etc.

How to Protect Employee from Unsafe Encrypted Traffic with Malware?

Solution

Secure Sockets Layer (SSL) encryption is growing tremendously worldwide, some popular examples of websites like dropbox and Gmail which are offering users the ability to have their entire sessions encrypted. But unfortunately, attackers are increasingly turning to encryption to evade detection which might bring some attacks, intrusions or malware. Enterprises face challenges as how to inspect incoming and outgoing traffic for threats under SSL encryption.

ZyXEL Next Generation USG Series featured with SSL inspection provides not only comprehensive security, but also deeper policy enforcement. It enables the USG's application intelligence, IDP, content filtering and anti-virus to inspect traffics in SSL encrypted connections and block threats that usually go unseen. ZyXEL USG Series could help to effectively meet the encrypted traffic management needs of enterprises, which when employee download a file from client by SSL, we are proud of optimizes securely delivered public cloud applications as well.
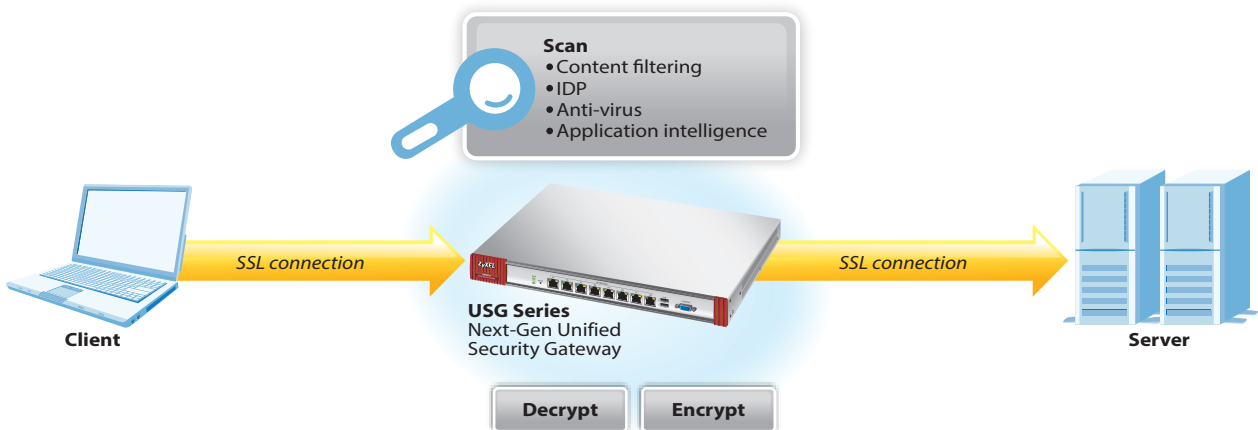
Performance Features

- SSL Ciphers are supported: RC4/DES/3DES/AES
- Protection including content filtering, IDP, anti-virus and application intelligence

Application Benefits

- Deeper policy enforcement
  - Apply application control policies even for SSL encrypted traffic
- Block invisible threats
  - Stop threats, bots and other malware that usually go unseen inside SSL encrypted traffic
- Comply with user privacy regulations
  - Create an exclude list to bypass traffic that is related to user privacy
  - Visible certificate cache list enables users to add items in the exclude list quick and easily
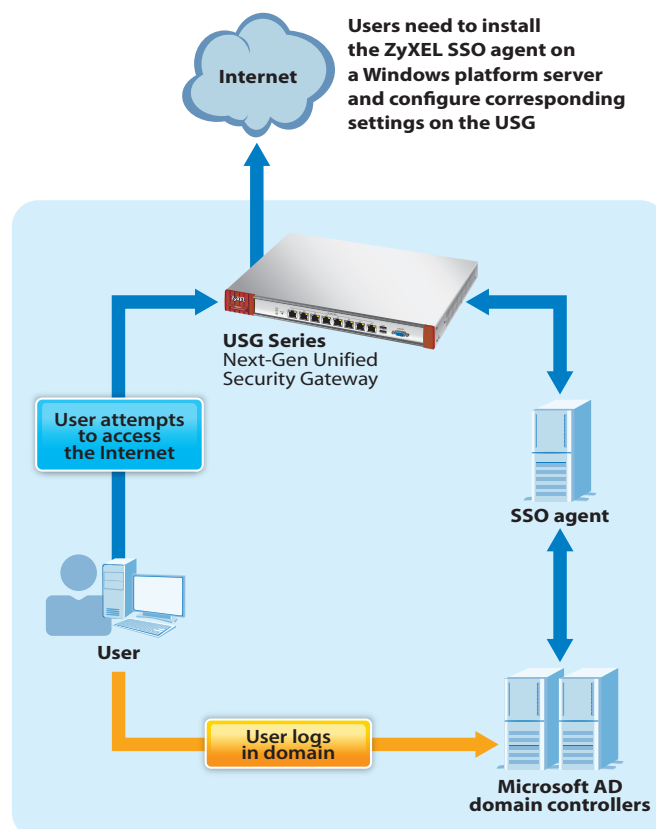
ZyXEL

How to Streamline User Authentication for Multiple Applications?

Solution

It is common in business daily operation that verification on users' identity is required before allowing them access the database, corporate email and ERP systems. Microsoft Active Directory (AD) is the most popular deployed authentication system. With the needs of Internet security protection, security appliances like USG series is added to the network with integration with Microsoft AD. Given this typical deployment, users need to give a user name and password not only when they join the network, but also when they attempt to run the Internet applications.

ZyXEL Next-Gen USG series supports single sign-on so users just need to sign in once to access both the Internet and all the resources and services integrated with Microsoft AD. The whole process is clientless implementation that users don't have to install any software on their PC. This enhances user experience by reducing password fatigue and time spent re-entering. It also relieves system administrators from help desk calls about passwords and eliminates efforts of injecting or replace some Microsoft AD components.


Internet

Users need to install the ZyXEL SSO agent on a Windows platform server and configure corresponding settings on the USG

USG Series Next-Gen Unified Security Gateway

User attempts to access the Internet

User

SSO agent

User logs in domain

Microsoft AD domain controllers

Performance Features

- Windows AD support
  - Windows 2008, 2008 R2, 2012
- SSO agent support
  - Windows 7 Pro, 2008, 2008 R2, 2012
- SSO agent supports up to 2 USGs, and receives user login info from up to 2 DCs

Application Benefits

- Transparent user authentication when users try to access various services (e.g. HTTP) through the ZyXEL USG series
- A single login is used to provide access to resources based on administrator-configured group memberships and policy matching
- Minimal administrator configuration is needed since on the users' machines nothing needs to be installed

How to Deploy and Expand a Managed Wi-Fi Network with Minimized Efforts?
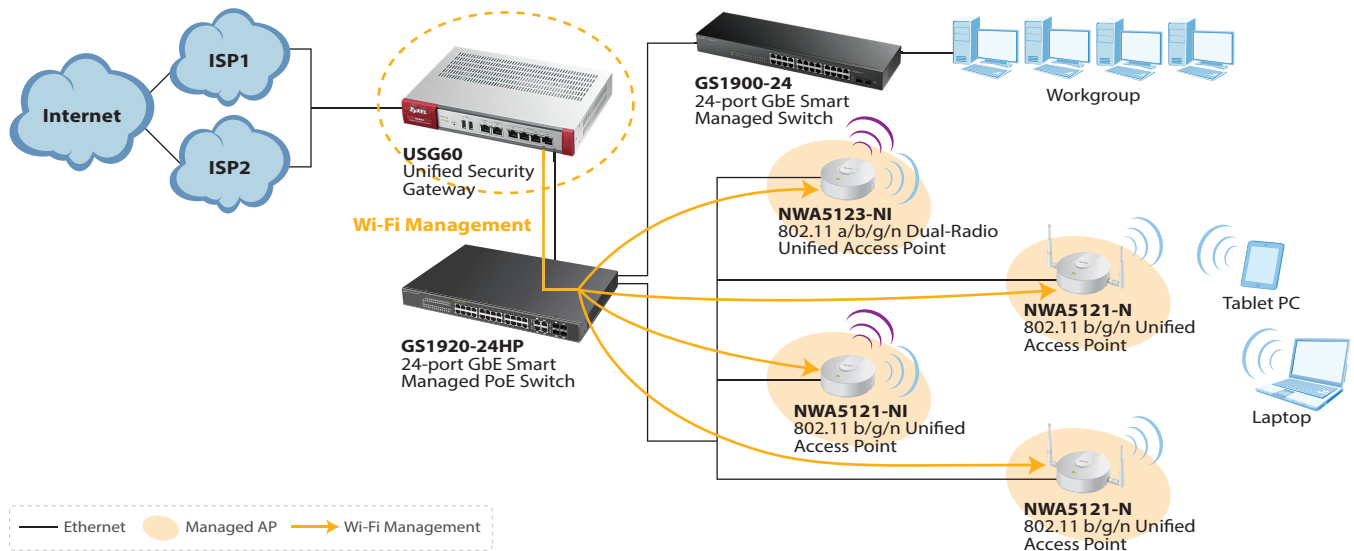
Solution

With the BYOD trend accelerating, Wi-Fi connectivity is now widely provided everywhere in office, meeting rooms and guest reception areas. This significantly and quickly increases demand for Wi-Fi access points, which in turn leads to more provisioning and management issues for network administrators. In fact, a well-designed WLAN controller is usually a solution to relieve administrators from these problems.

Now, ZyXEL makes its advanced AP Controller (APC) technology available to its complete Next-Gen USG ranges. This enables businesses to easily scale up the Wi-Fi networks with less investment and management efforts.

Performance Features

- Wireless L2 isolation
- Scheduled Wi-Fi service
- Dynamic Channel Selection (DCS)
- Client steering for 5 GHz priority and sticky client prevention
- Auto healing provides a stable and reliable coverage
- IEEE 802.1x authentication

- Captive portal Web authentication
- Customizable captive portal page
- RADIUS authentication
- Wi-Fi Multimedia (WMM) wireless QoS
- CAPWAP discovery protocol

Application Benefits

- Best TCO
  - Lower initial investment on equipment procurements
  - Less configuring and maintaining efforts on multiple devices
- Pay as You Grow
  - Scalable license-based Wi-Fi AP management for more flexibility
  - myZyXEL.com 2.0 offers a single friendly portal for managing the licensed services
- Comprehensive AP Portfolio
  - Wall mount, ceiling mount or even wall-plate installation for different needs
 - Indoor/outdoor wide-coverage installation for all locations

ZyXEL

How to Secure the Data Exchange among Several Offices?

Solution

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data transmissions across public networks like Internet. An IPSec VPN tunnel is usually established in two phases; in each phase, a security association (SA) is being established. A SA is a kind of agreement indicating the security parameters the USG and the remote IPSec router will use. In the first phase, an Internet Key Exchange (IKE) SA is established between the USG and the remote IPSec router; in the second phase, the IKE SA is used to securely establish an IPSec SA allowing the USG and the remote IPSec router to exchange data between computers on the local network and computers on the remote network.

USGs provide secure site-to-site communication between remote locations and corporate resources through the Internet. Using IPSec VPN, companies can build secure connections among branch offices, partners and headquarters as illustrated below.
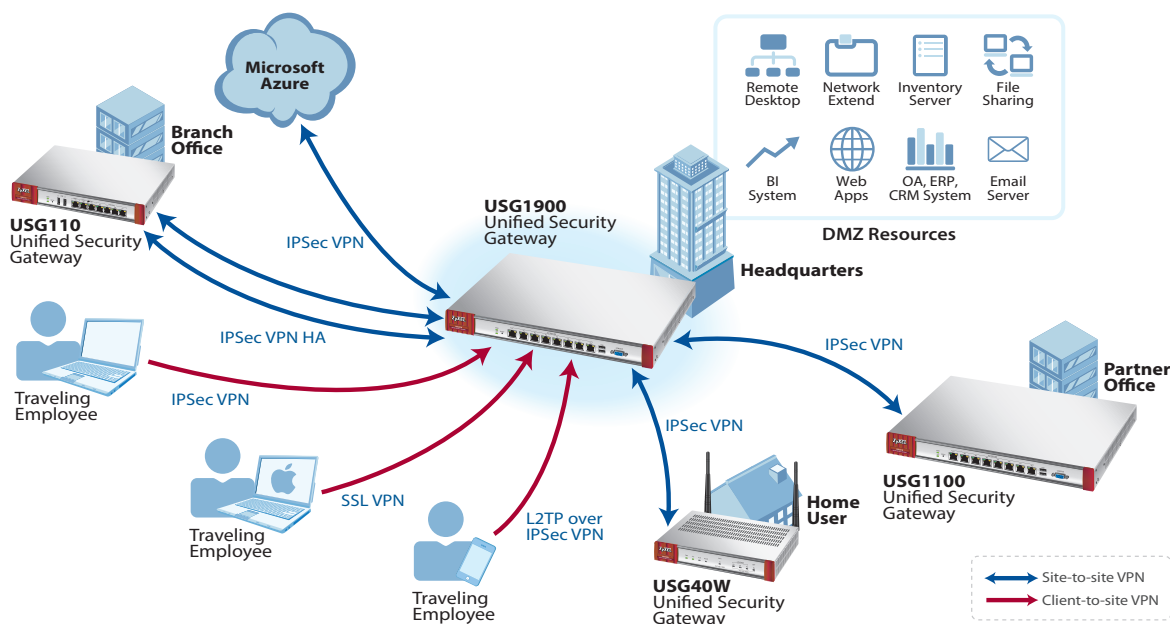
Performance Features

- ICSA-certified IPSec VPN
- Support algorithm: AES/3DES/DES, authentication: SHA-2/SHA-1/MD5
- Key management: IKEv1 and IKEv2 with EAP

Application Benefits

- A cost-effective solution for connecting branch offices or remote sites with the headquarters
- Securely encrypted connection over the Internet
- Connection is constantly available

16

How to Provide an Easy and Secure Remote Access for Traveling Employee?

Solution

Businesses from small to large all need to get ready for the growing demands of an increasingly mobile workforce and expanding distributed work sites, to compete in today's global market place. Secure remote access has become an imperative to business success.

ZyXEL provides comprehensive client-to-site solutions that perfectly work with ZyXEL USG or ZyWALL series for deploying easy-to-use, scalable and secured remote connections for mobile or distributed workers accessing back to corporate resources. The ZyXEL client-to-site VPN connections featured with comprehensive technologies, including SSL VPN, IPSec VPN and L2TP VPN, are adaptive to different client devices (PC or mobile phone) and different OS (Windows or MAC)

Performance Features

■ IPSec VPN

ZyXEL IPSec VPN client enables fast 3-step connection wizard that highly improve the user experience and let VPN connection is no longer a daunting task. The user-friendly interface makes it easy to install, configure and use.

■ SecuExtender SSL VPN

SecuExtender, the ZyXEL SSL VPN technology, works on both Windows and Mac operating systems. For Windows users, SecuExtender is free from pre-installation of a fat VPN client. ZyXEL security appliances will push VPN client and launch auto-installation while user logs in web-based authentication portal. For Mac users, a lite VPN software is provided to set up secured VPN connection.

■ L2TP VPN

ZyXEL USG/ZyWALL series supports build up L2TP over IPSec VPN connection with iOS and Android devices. iOS 4 and Android 2.2 above is supported.

Application Benefits

■ Enhanced layered security incorporating ZyXEL security appliances
■ Easy and intelligent installation reducing IT effort
■ Improved convenience and cost effectiveness
■ Secure business resource access anytime, anywhere

How to Ensure Trustworthy Site-to-site Communications for Remote Locations?
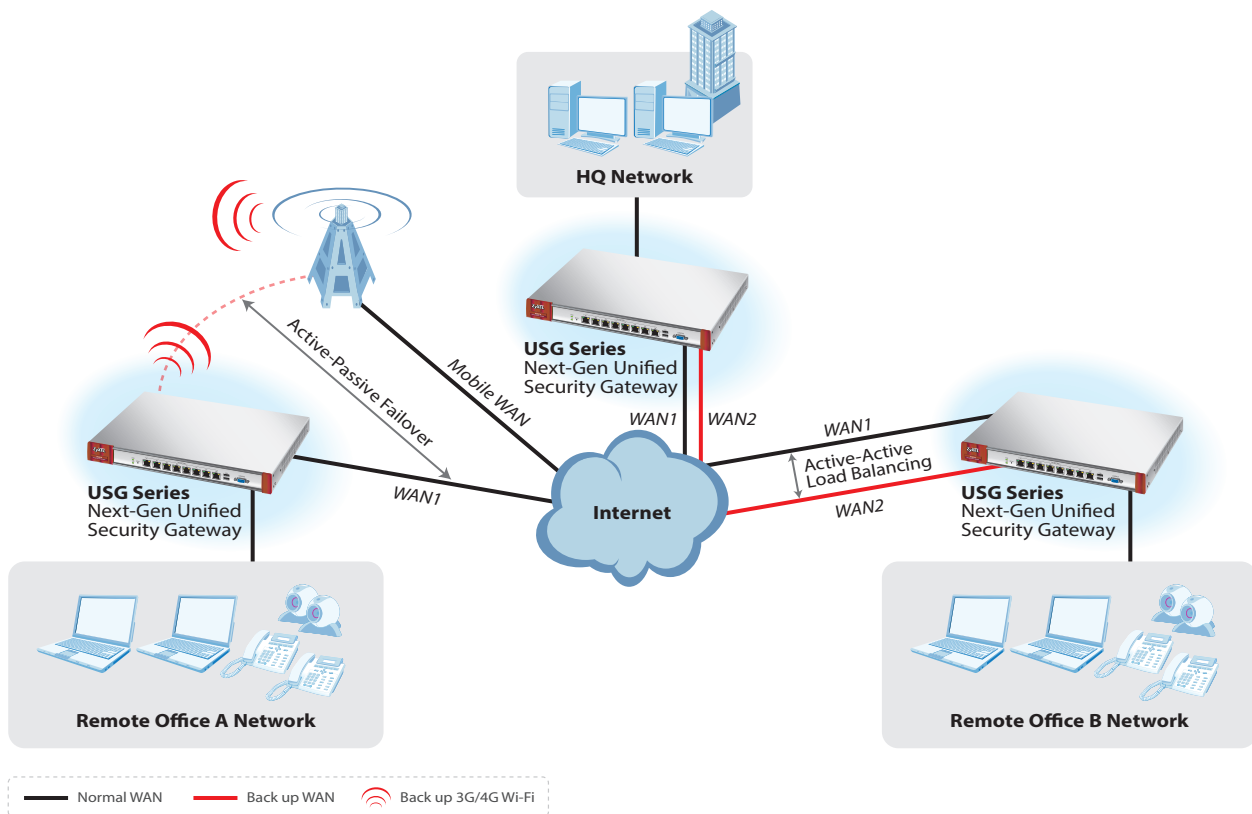
Solution

When the business grows and new regional offices are set up, the communications among these offices become a security concern to the IT team, especially when sensitive data like pricing or revenue numbers are delivered to and from these offices. In some retail business deployment, it is particularly important that these connections not only need to be secured also reliable in order to keep most precise data.

ZyXEL USG series not only supports site-to-site VPN, it also ensure the resiliency for mission-critical VPN deployments. The VPN high availability works in both active-active VPN load balancing and active-passive failover to suit the deployment needs.

Performance Features

- Utilizes GRE over IPSec and GRE trunk technology
- Support up to four (4) IPSec VPN tunnels for active-active VPN load balancing or active-passive failover

Application Benefits

- Highly available, secured site-to-site communications
- A cost-effective solution for small and medium-sized businesses to deploy resilient VPN connections; other than adopting expensive MPLS solution
- Aggregated bandwidth and load-balancing by enabling VPN connections in multiple WANs

Products at a Glance

USG1900/1100

Unified Security Gateway—Extreme Series

Uncompromising Security and Performance for Next Generation Business Needs

- Ultra-high performance Next Generation Firewall (NGFW) for medium to large businesses
- Enhanced manageability with unified security policy and Single Sign-On (SSO) support
- Multi-threat protection with firewall, Kaspersky anti-virus, anti-spam, content filtering, IDP, next-generation application intelligence, and SSL inspection
- Robust SSL, IPSec and L2TP over IPSec and IKEv2 VPN connectivity
- Built-in WLAN controller for centralized AP management and effortless WLAN scalability

USG310/210/110

Unified Security Gateway—Advanced Series

Delivering Next Generation Security with the Perfect Balance of Performance and Value

- Mid-range Next Generation Firewall (NGFW) for small and medium-sized businesses
- Comprehensive mobile bandwidth broadband dongle compatibility and multi-WAN load-balancing, failover and fall back support
- Built-in WLAN controller for centralized AP management and effortless WLAN scalability
- Multi-threat protection with firewall, Kaspersky anti-virus, anti-spam, content filtering, IDP, next-generation application intelligence, and SSL inspection
- Robust SSL, IPSec and L2TP over IPSec and IKEv2 VPN connectivity

USG60/60W/40/40W

Unified Security Gateway—Performance Series

Truly Integrated Security for Remote Offices, Retail Locations and Small Businesses

- Desktop Next Generation Firewall (NGFW) for small businesses
- Integrated single-radio (USG40W) or dual-radio (USG60W) wireless access point
- Multi-threat protection with firewall, Kaspersky anti-virus, anti-spam, content filtering, IDP, and next-generation application intelligence
- Robust SSL, IPSec and L2TP over IPSec and IKEv2 VPN connectivity
- Built-in WLAN controller for centralized AP management and effortless WLAN scalability

ZyXEL **one**network
Redefining network integration

ICSAlabs CERTIFIED IPSEC - BASIC

ICSAlabs CERTIFIED FIREWALL - SMB

POWERED BY ANTI-VIRUS

R6 READY

Next-Gen USG Quick Finder

Model	USG40/40W	USG60/60W	USG110	USG210	USG310	USG1100	USG1900
Description	**Performance Series**		**Advanced Series**			**Extreme Series**	
Firewall throughput	400 Mbps	1.0 Gbps	1.6 Gbps	1.9 Gbps	5.0 Gbps	6.0 Gbps	7.0 Gbps
VPN throughput	100 Mbps	180 Mbps	400 Mbps	500 Mbps	650 Mbps	800 Mbps	900 Mbps
UTM throughput (AV and IDP)	50 Mbps	90 Mbps	250 Mbps	300 Mbps	400 Mbps	500 Mbps	600 Mbps
Max. TCP concurrent sessions	20,000	40,000	60,000	80,000	100,000	500,000	500,000
Wi-Fi	802.11 b/g/n 2.4 GHz (USG40W)	802.11 a/b/g/n Concurrent 2.4 & 5 GHz (USG60W)	-	-	-	-	-
Managed AP number (default/max.)	2/10	2/10	2/18	2/18	2/18	2/18	2/18
Multi-WAN	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Unified security policy	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SSL inspection	-	-	Yes	Yes	Yes	Yes	Yes
Device HA	-	-	Yes	Yes	Yes	Yes	Yes
Port grouping	Yes	Yes	Yes	Yes	-	-	-
Single Sign-On (SSO)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Licenses and Accessories

Content Filtering

Content Filtering Service

Content Filtering allows administrators to easily block certain types of web content without having to manually block each URL individually. Block inappropriate sites and social networking sites quickly and easily.

Anti-Virus

Anti-Virus Service (powered by Kaspersky)

Anti-Virus (AV) is the first line of defense to protect your internal network against zero-day attacks and the most active viruses in the wild list. ZyXEL security appliances integrate the world-leading AV technology from the industry leader Karspersky to guard the networks of our customers. Gateway Anti Virus shouldn't be ignored even client AV installed, due to client AV can be disabled by users or it cannot be installed in all the end devices in the network. The ZyXEL AV provides an additional layer of defense against latest threats, buying valuable time for software clients to be updated to an appropriate protection level.

Anti-Spam

Anti-Spam Service

Anti-Spam service protects against spam, phishing and virus-laden emails. The extremely high performance technology comes from the unique recurrent pattern detection (RPD) mechanism that possesses its superior capability through analyzing millions of new patterns each day (24x7x365) to block all the associated messages real-time. In addition, the USG applies sender-based IP reputation to remove over 80% of unwanted mails and to take advantage of the zero-hour virus outbreak protection feature, which is capable of blocking or delaying suspicious messages hours before commercial anti-virus signatures are available.

Intrusion Detection & Prevention

IDP Service

ZyXEL Intrusion Detection and Prevention (IDP) allows the administrator to control specific applications and also block well known trojans and back door applications that can infiltrate your internal network. The ZyXEL IDP system uses Deep Packet Inspection (DPI) technology and supports up to 8,000+ signatures for the top well known applications and Trojan/backdoor applications. This adds another layer of security and also provides the administrator the flexibility to block specific programs that are not allowed on the network like P2P file sharing or instant messaging.

Application Intelligence

Application Intelligence

ZyXEL Application Intelligence utilize the DPI engine and enables administrators the capabilities to identify, categorize and control over 3,000 social, gaming, productivity, and other Web applications and behaviors. Administrators can prioritize productive applications, throttle acceptable ones, and block unproductive applications to boost productivity and prevent bandwidth abuse.

VPN

SSL VPN Client Service

Browser-triggered, easy implementation without requiring client software to be pre-installed*

(*) Client-less installation is only supported in Windows-based OS. In MAC OS the pre-installation of client software is still required.

IPSec VPN Client Service

Deploying client to site VPN connection via client software approach, with strongest industry authentication support (SHA-2 512-bit) and fast connection

Integrated WLAN Controller

Managed AP Service

Wi-Fi access has been the mandatory in deploying a modern network. With the increase of connected end devices, the network administrator will need to add more Wi-Fi AP to the network. By incorporating the managed AP service in the Next-Gen USG series, administrators can apply the centralized management and provisioning to the newly added Wi-Fi APs.

Security Licenses

Product	Kaspersky Anti-Virus	IDP	Content Filtering	Anti-Spam
USG1900	1 year 2 years	1 year 2 years	1 year 2 years	1 year 2 years
USG1100	1 year 2 years	1 year 2 years	1 year 2 years	1 year 2 years
USG310	1 year 2 years	1 year 2 years	1 year 2 years	1 year 2 years
USG210	1 year 2 years	1 year 2 years	1 year 2 years	1 year 2 years
USG110	1 year 2 years	1 year 2 years	1 year 2 years	1 year 2 years
USG60(W)	1 year 2 years	1 year 2 years	1 year 2 years	1 year 2 years
USG40(W)	1 year 2 years	1 year 2 years	1 year 2 years	1 year 2 years

Notes:
1. ZyXEL USGs can be purchased with bundled 12-month standard license (anti-virus, anti-spam, content filtering and IDP) with extra 1-month trial.
2. Licenses can be easily activated, renewed and managed at myZyXEL.com 2.0 3. License bundles may vary according to region. Please contact your local sales representative for more information.
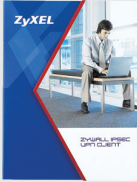
VPN, Management and Reporting Licenses

Product	SSL VPN Tunnels	SecuExtender—SSL VPN Client[*1]	IPSec VPN Client	Managed APs[*2]	Vantage Report
USG1900	Add 5 Tunnels Add 10 Tunnels Add 50 Tunnels	For 1 client For 5 clients For 10 clients	For 1 client For 5 clients For 10 clients For 50 clients	Add 8 APs	For 1 device For 5 devices For 25 devices For 100 devices
USG1100					
USG310					
USG210					
USG110					
USG60/60W	Add 5 Tunnels Add 10 Tunnels				
USG40/40W					

Notes:
*1: Support OS: MAC OS 10.7 or later
*2: With firmware ZLD 4.10 or later

Access Point Compatibility List

Series	NWA5120 Series	NWA5000 Series	NWA3000-N Series
	Unified Access Point	Managed Access Point	Unified Pro Access Point
Models	NWA5121-NI NWA5121-N NWA5123-NI	NWA5160N NWA5560-N NWA5550-N	NWA3160-N NWA3560-N NWA3550-N
Functions			
Central management	Yes	Yes	Yes
Auto provisioning	Yes	Yes	Yes
Data forwarding	Local bridge	Local bridge	Local bridge

Accessories

Item	Description	Supported OS
IPSec VPN Client	IPSec VPN client software for the ZyWALL and USG Series with Easy VPN for zero-configuration remote access	• Windows XP (32-bit) • Windows Server 2003 (32-bit) • Windows Server 2008 (32/64-bit) • Windows Vista (32/64-bit) • Windows 7 (32/64-bit) • Windows 8 (32/64-bit)
SecuExtender— SSL VPN Client	SSL VPN client software for the ZyWALL and USG Series with auto-installation in Windows, and lite set up for MAC user	• Windows OS • MAC OS 10.7 or later

Notes:
1. A 30-day trial version of IPSec VPN client and SSL VPN client for MAC OS can be downloaded from official ZyXEL website. To continue using the application,
   please contact your regional sales representatives and purchase a commercial license for the application.
2. SSL VPN client for Windows OS is pushed from USG/ZyWALL device and launches automatically. It does not require a license key to activate the application.

ZyXEL

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 23 555 3689
Fax: +31 23 557 8492
Email: sales@zyxel.nl
http://www.zyxel.nl
http://www.zyxel.be

**ZyXEL Bulgaria
(Bulgaria, Macedonia,
Albania, Kosovo)**
Tel: +3592 4443343
Email: info@cz.zyxel.com
http://www.zyxel.bg

ZyXEL Czech Republic
Tel: +420 241 091 350
Hotline: +420 241 774 665
Fax: +420 241 091 359
Email: sales@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 1 848 0690
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: +48 223 338 250
Hotline: +48 226 521 626
Fax: +48 223 338 251
Email: info@pl.zyxel.com
http://www.zyxel.pl

ZyXEL Romania
Tel: +40 31 0809 888
Fax: +40 31 0809 890
Email: info@cz.zyxel.com
http://www.zyxel.ro

ZyXEL Russia
Tel: +7 (495) 539-9935
Fax: +7 (495) 542-8925
Email: info@zyxel.ru
http://www.zyxel.ru

ZyXEL Slovakia
Tel: +421 220 861 847
Hotline: +421 220 861 848
Fax: +421 243 193 990
Email: info@cz.zyxel.com
http://www.zyxel.sk

ZyXEL Communications ES Ltd
Tel: 911 792 100
Email: ventas@zyxel.es
http://www.zyxel.es

ZyXEL Sweden A/S
Tel: +46 8 55 77 60 60
Fax: +46 8 55 77 60 61
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: +7-727-2590-699
Fax: +7-727-2590-689
Email: info@zyxel.kz
http://www.zyxel.kz

ZyXEL Korea Corp.
Tel: +82-2-890-5535
Fax: +82-2-890-5537
Email: sales@zyxel.kr
http://www.zyxel.kr

ZyXEL Malaysia
Tel: +603 2282 1111
Fax: +603 2287 2611
Email: sales@zyxel.com.my
http://www.zyxel.com.my

ZyXEL Middle East FZE
Tel: +971 4 372 4483
Cell: +971 562146416
Email: sales@zyxel-me.com
http://www.zyxel-me.com

ZyXEL Philippine
Email: sales@zyxel.com.ph
http://www.zyxel.com.ph

ZyXEL Singapore
Tel: +65 6339 3218
Hotline: +65 6339 1663
Fax: +65 6339 3318
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

ZyXEL Vietnam
Tel: (+848) 35202910
Fax: (+848) 35202800
Email: sales_vn@zyxel.com.tw
http://www.zyxel.com/vn/vi/

■ The Americas

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

ZyXEL Brazil
Tel: +55 (11) 3373-7470
Fax: +55 (11) 3373-7510
Email: comercial@zyxel.com.br
http://www.zyxel.com/br/pt/

For more product information, visit us on the web at www.ZyXEL.com

5-000-00815002   10/15