

The ZyXEL logo is displayed in white, bold, sans-serif font on a blue rectangular background.

Security on a New Level



**ZyWALL USG
Series**
Application Guide

The Future Is Ahead.
Stay Ahead with ZyXEL USGs.









Table of Contents

Editorial	4
The Chain Store	6
Scenarios	8
Ensure Non-stop Connectivity to the Internet	8
Get Internet Connections Utilized Effectively	9
Connect and Migrate to IPv6 Smoothly	10
Provide Internet-connected Servers and Avoid Security Breach from Web Activities	11
Secure the Data Exchange among Several Offices	12
Protect the Accessing Traffics from Remote Workers	13
Offer Remote Access with Managed Access Right via Web Browser	14
Enjoy the Secure Remote Access with Mobile Devices	15
Ensure Critical Application Traffics while Giving Key Users the Highest Bandwidth Priority	16
Ensure Employee Productivity	17
Protect Employee from Unsafe Web Sites with Potential Malware Attacks	18
Protect Business from Spams	19
Products at a Glance	20

Editorial

Dear Resellers,

It's been over a year since we presented our new ZyWALL USG 20/20W/50 Series completing the whole USG product line with the commercial segment models. Since then we have sold more than 20,000 pcs of these new devices and the numbers are still growing every month. With other words, our transition from the old ZyNOS platform to the new ZLD based platform has been an enormous success. However there is no reason to put our feet up as we have also seen over the last years a monthly increase in security threats. This is a huge challenge for every security vendor.

Taking the situation described above into consideration, I am now even more pleased to be able to announce the introduction of the next major firmware release for the USG Series: the ZLD 3.0. This is so important, because we have used the year 2011 to develop a firmware which directly addresses all the threats and malware elements we have identified in the previous years. And I can only emphasize the result provided by our R&D team is stunning. Malware protection – one of the key threats in today's security arena – has been massively improved by adding new services to the USG. In cooperation with Commtouch – one of the leading security technology providers – we have added one of the most advanced Anti-Spam solutions to the ZyWALL

USG Solution portfolio. Rather than evaluating the content of messages, the Commtouch Anti-Spam analyzes billions of emails in real-time, recognizing and protecting against new spam outbreaks the moment they emerge. Another service addition is the Content Filter Solution from Commtouch. Here again we see industry leading technology helping us to make the best out of our ZyWALLs.

When we set up the first USG application guide in 2010 the basic consideration was that we wanted to build a guide for our huge customer base of small and mid-sized resellers. This aim has not changed. Thousands of such resellers have helped us to make our new products successful and from the feedback we have received over the whole year we could easily see that our application guide has supported this success in an excellent way. For the ZLD 3.0 we see a lot of attractive new features coming out: a greatly improved throughput rate, IPv6 capabilities to ensure future investments, the already mentioned new malware protection services, VPN and infrastructure enhancements and much more. And the best part – you do not need to pay a single penny for these improvements. As always, the firmware upgrade remains free of charge.



Last time we shared the challenges of a general manager of a chocolate factory. However we see that the integration of branch offices, home offices and road warriors is increasing including growing expectations on the IT to build up such distributed networks smoothly and most important of all secure. This is why, this time, we picked the example of a chain store.

We hope that this guide will help you to advise your customers in the best possible way. Our application guide aims at supporting you in finding the right solution for your SB customers, helping you 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. Please also refer to the newly established product finder, which helps you to tailor the solutions according to your customer's specific needs. Here's to successful cooperation!

Best regards,



Thorsten Kurpjuhn
Market Development Manager
t.kurpjuhn@zyxel.de



Justin Lin
Product Line Manager
Justin.Lin@zyxel.com.tw

The Supermarket Chain Store



A middle-sized supermarket in Asia has five stores and provides online shopping services. The company has currently hired twenty employees and opened five stores with seven more employees each. The executive plans to recruit several remote workers and some freelance employees such as photographers or designers, and these freelance workers occasionally need to access company resources. This company is facing a series of challenges that can probably be solved following this guide.

Challenge:

Internet downtime causes losses to our company. We really need reliable, continuous Internet access!

Solution:

Multiple WANs allow your company to stay online. Use redundant Internet connections or 3G as a backup, and no more suffer from downtime again.

See more on page 8

Challenge:

Our Internet access is deployed by several different Internet access providers and we would like to utilize the bandwidth efficiently to guarantee our customers with smooth, non-stop online shopping services.

Solution:

The WAN load balancing and inbound load balancing mechanisms distribute traffic loads according to the WAN status. This improves quality of services and maximizes bandwidth utilization as well.

See more on page 9

Challenge:

Internet service providers with IPv6 deployments are increasing. We would like our company to have a future-proof upgradability to IPv6.

Solution:

Choosing a security appliance with “IPv6-ready” certification can protect your investment. It ensures businesses of a smooth migration to IPv6 with ZyWALL USG’s ability to identify and process IPv6 traffics.

See more on page 10

Challenge:

We would like our customers to be able to download our brochures and to visit our Web site without provoking security breaches.

Solution:

Network Address Translation (NAT) allows customers to easily access FTP or Web servers while protecting your network from attacks.

See more on page 11

Challenge:

Our company has five stores, and we would like to securely integrate them into our company network.

Solution:

IPSec VPN enables you to establish secure tunnels via the Internet. This allows your staff in branch offices to access the company network the same way as anyone working in the main office. Just install a ZyWALL USG on each location and establish a secure connection with the headquarters instantly.

See more on page 12

Challenge:

Excellent! So how about our sales team or other remote workers? Do they need a firewall too? We are looking for an inexpensive and easy solution for them as well.

Solution:

With the IPSec client software, you can enable clients to build a client-to-site connection to your office. Moreover, the “EASY VPN” solution is also easy for clients to install software without configuration efforts.

See more on page 13

Challenge:

Our company works with several freelancers who only need occasional, managed access to our network. What would you suggest?

Solution:

SSL-VPN is the solution. Freelancers can easily use their browsers to access the ZyWALL USG and build a secure tunnel (using the same technology as online banking) with no special software required. This is an easy, inexpensive way to access the company network for people who need only occasional access to company resources.

See more on page 14

Challenge:

Access to network applications using mobile devices such as smartphones and tablets are more and more common nowadays. We would like to provide this service to our employee and customers.

Solution:

L2TP VPN is designed for remote users with mobile devices to securely connect to the network. Security appliances supporting L2TP VPN technology allow employees in remote areas to access the headquarters easily and freely.

See more on page 15

Challenge:

Our company uses VoIP to reduce telephone costs. How can we get excellent voice data quality? And how can we give the highest bandwidth priority to key users like important executives?

Solution:

Bandwidth management functions enable you to not only prioritize VoIP or any other traffic to ensure the highest quality with neither delay nor jitter but also assign a certain bandwidth to each user, so you and other important executives can have absolute priority on the network.

See more on page 16

Challenge:

We have noticed that more and more of the employees are using IM, P2P and social network applications. We'd like to have control over this, so they can focus on their works and avoid abusing the office Internet connection, and therefore the consequential loss of the company.

Solution:

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

See more on page 17

Challenge:

The World Wide Web has become the main target of network threats, since the Internet itself is a very effective malware delivery mechanism. We would like to protect our employee from malware attacks.

Solution:

Content filtering offers you a large diverse community, constant threat discovery, blocking of unknown Web contents, real-time analysis and immediate signature updates to protect business from Web threats including malware and phishing.

See more on page 18

Challenge:

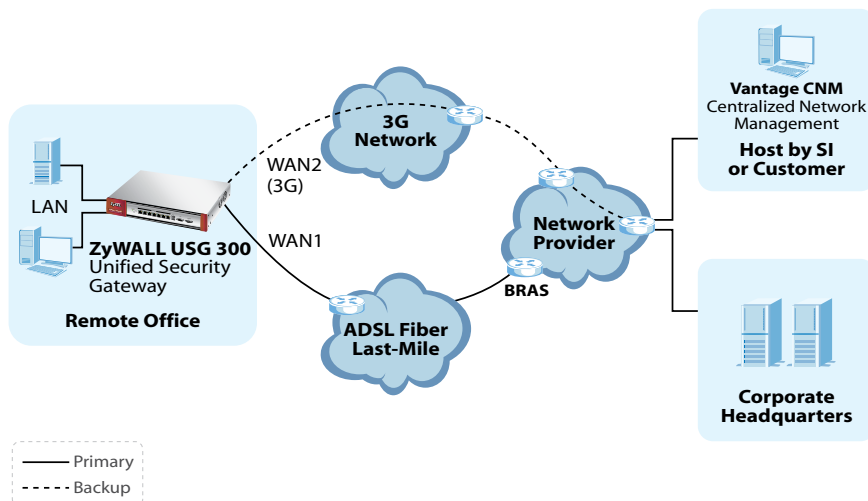
We get a large number of spam emails daily from improperly configured or virus-infected email servers. This causes significant productivity loss to our business.

Solution:

The Anti-Spam service is a feature that marks or discards unsolicited commercial or junk e-mails. It's a great solution with advanced mechanisms designed for excellent performance and extremely high detection rates.

See more on page 19

How to Ensure Non-stop Connectivity to the Internet?



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 multiple WAN feature of ZyWALL USG Series enables users to connect to up to two ISPs or networks via Ethernet, PPPoE or 3G. Users can either use trunks for WAN traffic load balancing to increase the overall network throughput or use it as a backup to enhance network reliability.

Performance Features

- Multiple WAN ports for load sharing and failover
- Non-stop Internet access with multiple WAN and 3G backups
- Supports to 2 modes:
 - active-active for load sharing
 - active-passive for failover
- A broad range of 3G cards are supported (For the list of currently supported models, please visit www.zyxel.com)

Load balancing will be further described in Scenario 2. Here we will demonstrate the scenario for unlimited Internet access with PPPoE as the primary WAN, and perform 3G backups through USB; that is, the USG normally uses the PPPoE interface for Internet access and will switch to the 3G interface if the PPPoE connection fails.

Application Benefits

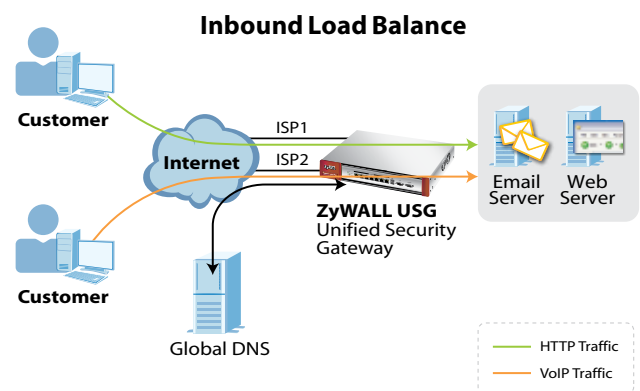
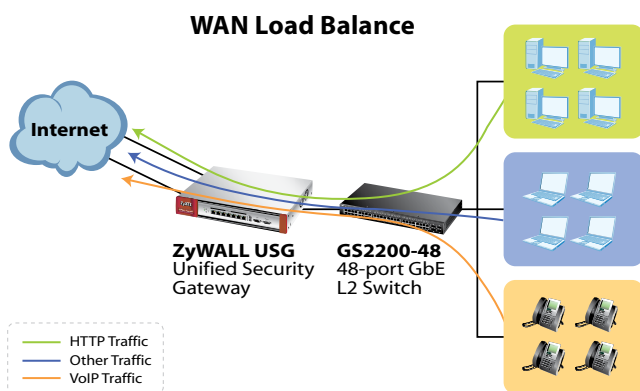
- Keep your business connected even when the Internet goes down
- Flexible 3G backup as a WAN alternative to increase availability
- Smooth, highly reliable network connectivity

How to Get Internet Connections Utilized Effectively?

Solution

As a business network gateway, the ZyWALL 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.



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

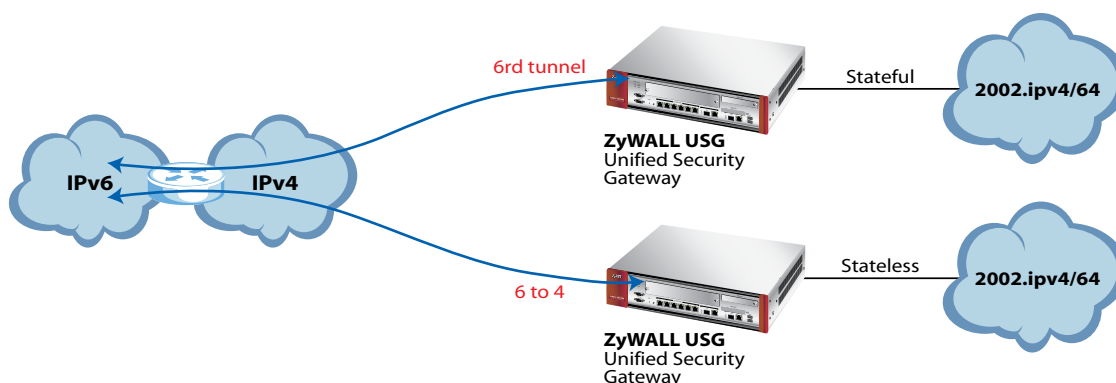


How to Connect and Migrate to IPv6 Smoothly?

Solution

The ZyWALL USG Series is IPv6-ready today and has met the requirements of "IPv6 Ready" Phase-1 and Phase-2 as specified by the IPv6 Forum, a world-wide consortium providing technical guidance for IPv6 deployments.

With IPv6 feature enabled, the USG can assign an IPv6 to connected clients and pass IPv6 traffics through the IPv4 environment. The USG Series supports dual-stack and IPv4 tunneling (6rd and 6to4 transition tunnel) implementations for Internet connectivity to access IPv6 applications.



Performance Features

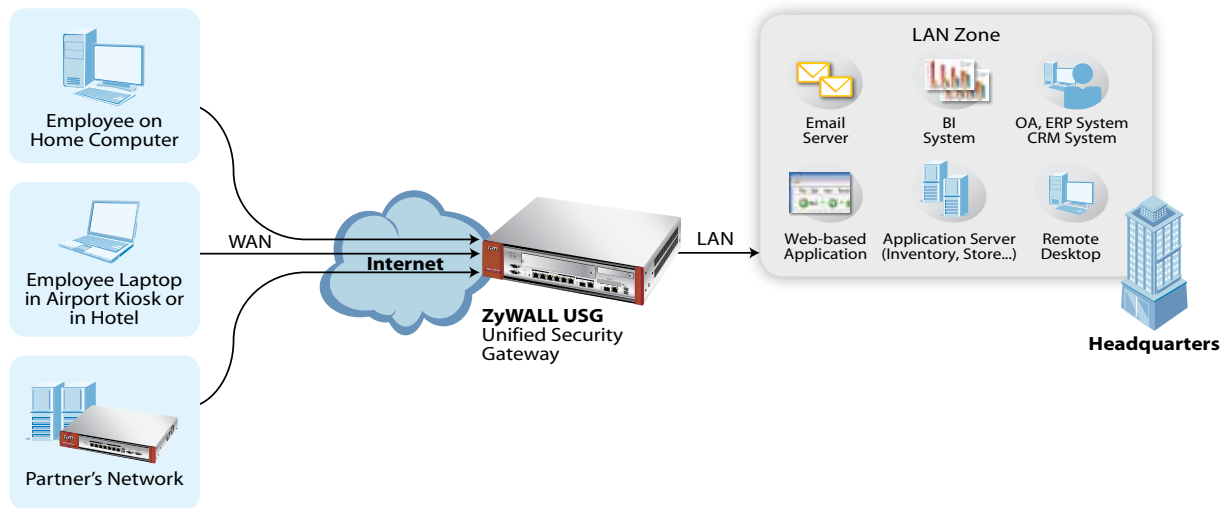


- "IPv6 ready" certified
- Supports IPv6 dual stack, 6rd (IPv6 Rapid Deployment) and 6to4 transition tunnel for WAN
- Supports IPv6 stateless and stateful, DHCPv6 for LAN
- Supports IPv6 firewall

Application Benefits

- Meeting industry standards
- Smooth migration from IPv4 to IPv6
- Investment protection

How to Provide Internet-connected Servers and Avoid Security Breach from Web Activities?



Solution

Network Address Translation (NAT) performs translation to the IP address of a host in a packet. The NAT feature allows computers on a private network behind the ZyWALL USG to be accessible from outside.

Placing servers behind a USG offering maximum network protection while allowing the WAN-side clients/servers to access intranet servers is common practice. A company may have an FTP server that needs to be accessible by remote workers over the Internet. To fulfill this requirement, the administrator can configure a NAT mapping rule to forward the traffic from the Internet to intranet.

Performance Features

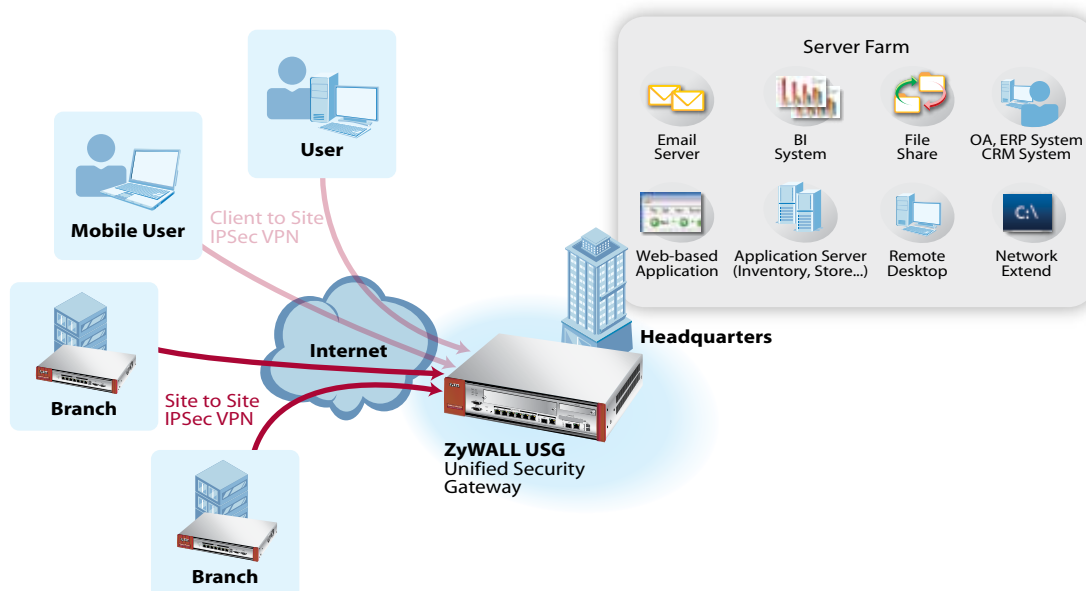
- Supports NAT/PAT and Policy-based NAT (SNAT)
- Supports one-to-one, many-to-one and NAT loopback

Application Benefits

- Ensured service availability
- Hiding the server's real IP address to avoid attacks



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 ZyWALL 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.

ZyWALL 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-1/MD5

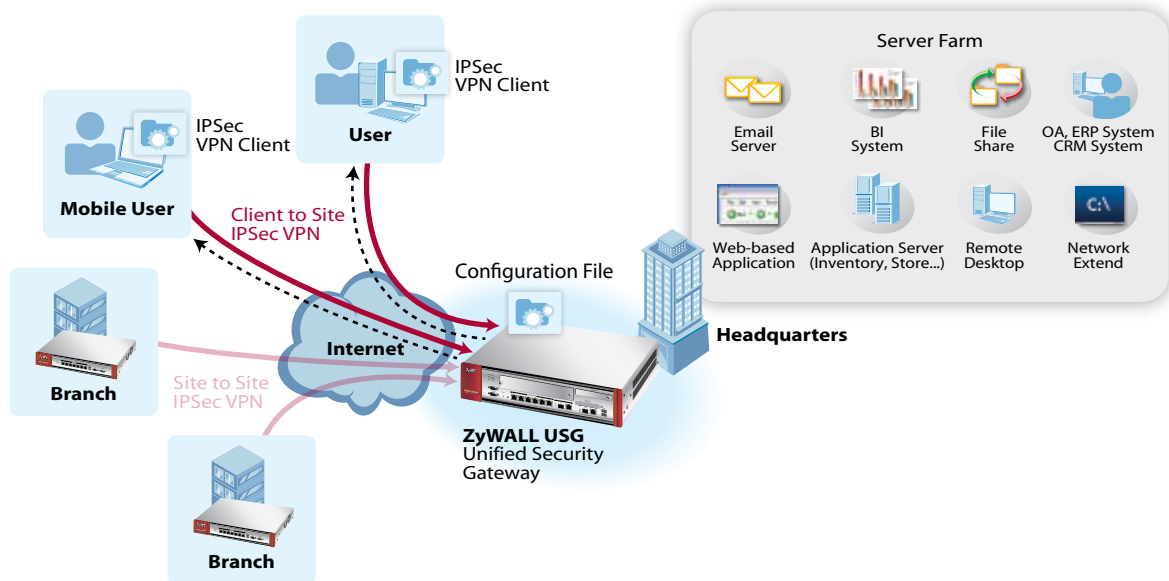
Application Benefits

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

How to Protect the Accessing Traffics from Remote Workers?

Easy provisioning for ZyWALL IPSec VPN client

- USG automatically provides configuration file to the client.



Solution

Remote workers and telecommuters can use SSL or IPSec VPN to safely access the company network without having to install VPN software. The ZyWALL USG Series provides a flexible and easy way to enable remote workers, vendors and partners to securely access your network resources, improving both security and efficiency. The USG Series is suitable for organizations of any size. Using IPSec VPN, any company can establish secure connections to its branch offices, partners and headquarters.

Although establishing a VPN tunnel is a viable solution for the purpose, however it is difficult for non-technical employees like sales people due to the complicated configuration. Equipped with the "EASY VPN" solution, the USG can automatically push the configuration files to provision the VPN clients; this eliminates the configuration efforts while securing the access at the same time.

Performance Features

- Auto provisioning for IPSec VPN
- Pre-configured for mass deployment
- EASY VPN compatibility with all ZyWALL USG

Application Benefits

- Zero-configuration remote access
- Lower administration overhead
- User friendly – just install, reboot and go



How to Offer Remote Access with Managed Access Right via Web Browser?

Solution

SSL-VPN is the solution. Freelancers can easily use their browsers to access the ZyWALL USG and build a secure tunnel (using the same technology as online banking) with no software required. This is an easy, inexpensive way to access the company network for people who need only occasional access to the company resource.

The ZyWALL USG Series provides a SSL VPN function that enables telecommuters to easily access company resources via a secure VPN tunnel, and all they need on their PC is a browser. Besides, SSL VPN also enables network administrator to define individual access rules that allow different user profiles to obtain access privileges to different company resources. For instance, a network administrator can set up a SSL VPN rule to allow an authorized manager to remotely control company servers with RDP or VNC through SSL VPN tunnels. The administrator can also set up a SSL VPN rule to allow the sales team to remotely access the shared files needed for daily tasks.

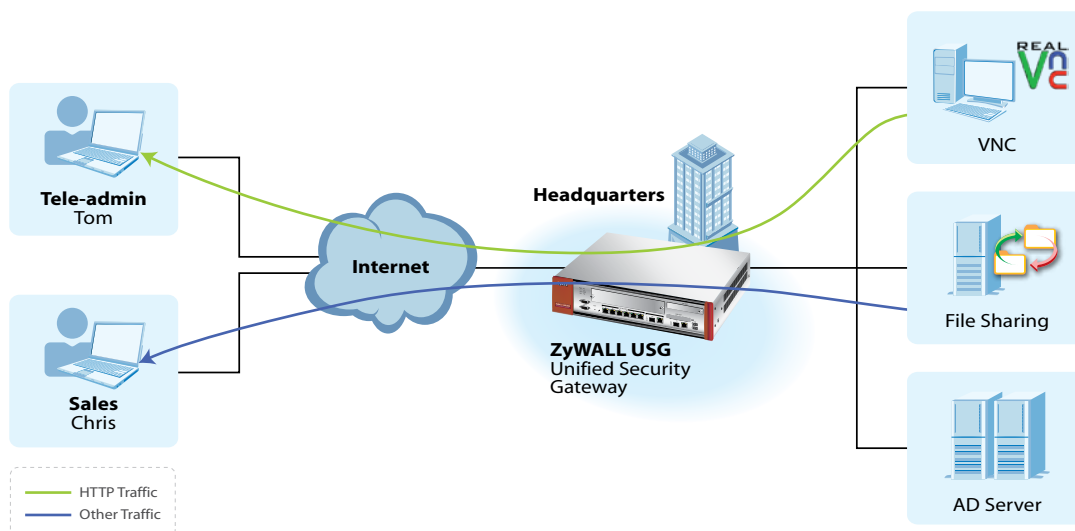


Performance Features

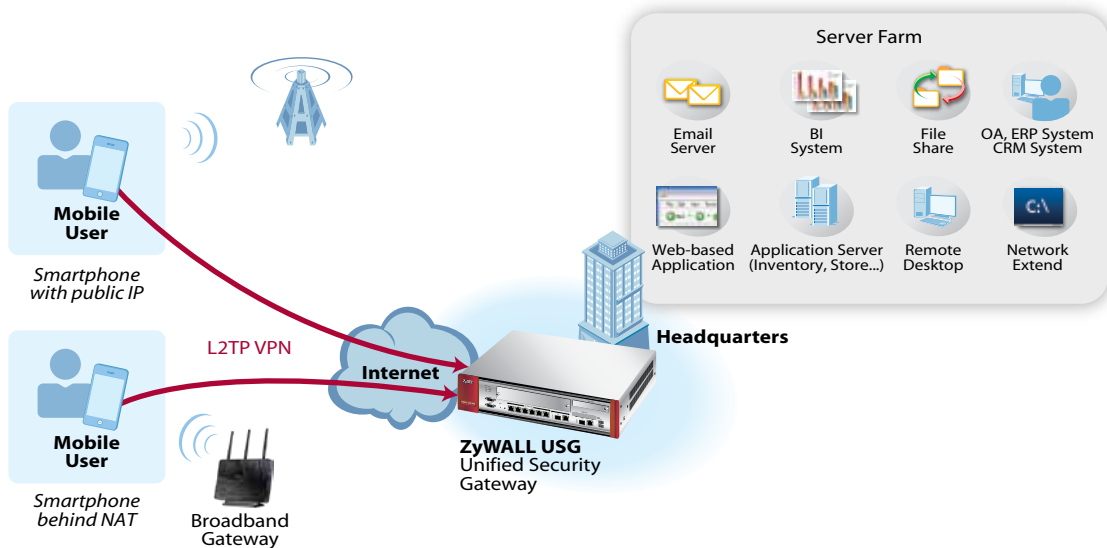
- Clientless secure remote access
- Supports two SSL VPN network access modes: reverse proxy and full tunnel
- Customizable user portal
- Easy to use with a Web browser

Application Benefits

- Less administrative overhead and technical support required than traditional VPN clients
- Easier to set up and troubleshoot



How to Enjoy the Secure Remote Access with Mobile Devices?



Solution

L2TP VPN is designed for remote users with mobile devices to securely connect to the network behind the ZyWALL USG. The remote users do not need their own IPSec gateways or VPN client software.

The ZyWALL USG Series supports L2TP VPN technology on iPhone/Android phones and many other mobile devices; this enables employee in remote areas to access the headquarters very easily and freely. A USG can work with iOS/Android mobile devices to establish VPN connection to provide secure, private data exchange even if the mobile devices are behind the NAT.

Performance Features

- L2TP over IPSec for iOS and Android
- Supports iOS 4 and iOS 5
- Supports Android 2.2 and 2.3



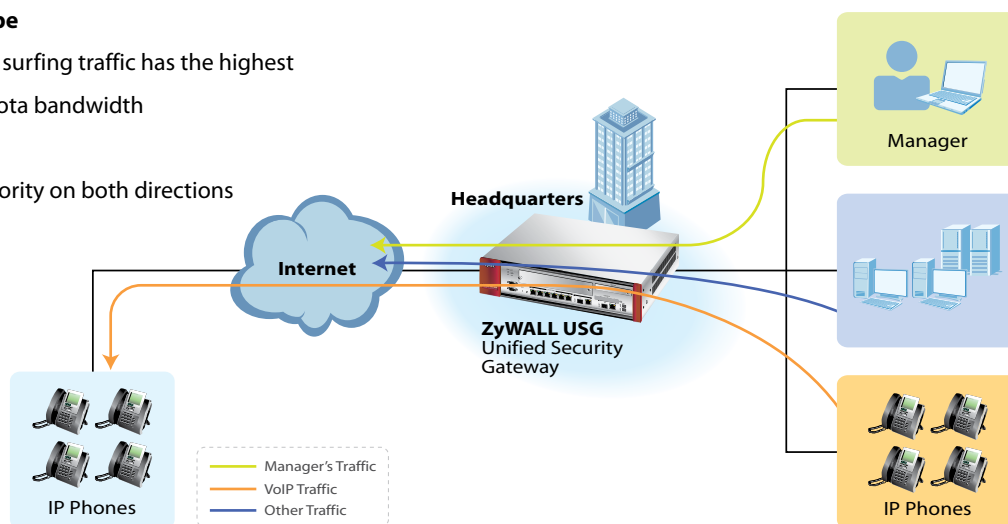
Application Benefits

- Improved convenience
- Improved cost effectiveness
- Secure business resource access anytime, anywhere

How to Ensure Critical Application Traffics while Giving Key Users the Highest Bandwidth Priority?

Managed by user or traffic type

- Guarantee managers' internet surfing traffic has the highest priority and with a specific quota bandwidth
- Limit session per host
- VoIP traffic has the highest priority on both directions



Solution

There are various types of traffics on a company network. Since the bandwidth is always limited, some traffic needs higher priority to ensure the required operating efficiency; and some users in charge of important tasks also need higher priority over the others as they depends more on reliable data transmission.

The ZyWALL USG Series provides the Bandwidth Management (BWM) function to effectively manage bandwidth with flexible criteria. For instance, since the VoIP traffic is prone to delay and jitter, it usually gets the highest priority on any company network for its time-sensitive nature. In addition, the Bandwidth Management function gives the top executives the highest Internet traffic priority by reserving a certain bandwidth for each particular user of the level. Furthermore, network administrators should set up a limit during the working hours to limit each user within a certain number of sessions to prevent them from consuming too much company bandwidth.



Performance Features

- Bandwidth Management
- VoIP traffic classes are guaranteed to receive a specified minimum amount of available bandwidth
- Employees with higher priorities are guaranteed to enjoy smooth Internet experience

Application Benefits

- Excellent Quality of Service (QoS) for VoIP
- Priority access for dedicated users
- Efficient usage of company bandwidth
- Minimize the network connection cost with Bandwidth Management

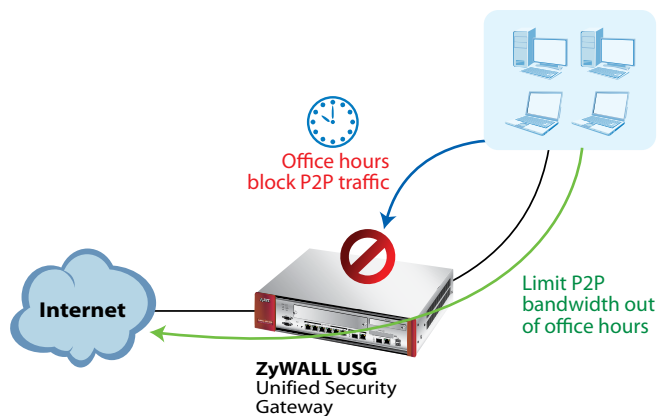
How to Ensure Employee Productivity?



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 Control” function on the ZyWALL USG Series, you have granular control of IM, P2P 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 time period and a maximum available bandwidth. (IM/P2P requires an IDP service license).



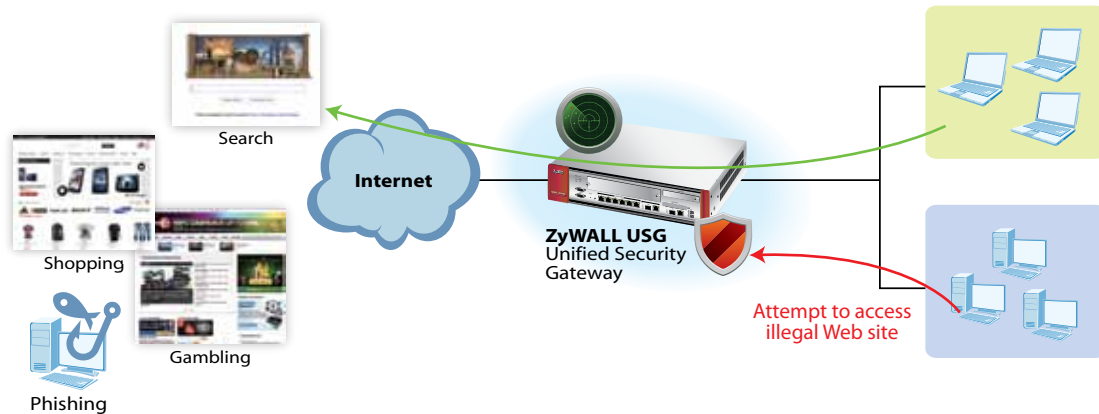
Performance Features

- Granular access control over applications, IM/P2P, stream-based media and VoIP
- Supports more than 15 catalogues of IM and P2P
- Maximum/guaranteed bandwidth
- Application Patrol supported by ZyWALL USG 2000/1000/300/200/100/50

Application Benefits

- Save money and increase productivity
- Granular control over each user’s access privilege
- Less danger from Internet abuse
- Full control over the company network

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



Solution

The content filter built into the ZyWALL 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.

- Identify new Web threats in real time: a deep, real-time inspection of the content, URLs, IP addresses and protocols is performed by cloud-based tools and researchers.
- Improved security efficiency and operations: the cloud-based community security is designed for incident prevention and threat analyzing, rating and blocking before they can penetrate networks and infect systems.

Powered by Blue Coat and Commtouch, the leading technology provider, ZyXEL’s Content Filter Solution can reduce costs and extend protection by combining a comprehensive, continuously integrated database featuring millions of URLs, IP addresses and domains.

Performance Features

- Optional Content Filtering services from Blue Coat and Commtouch
- Web 2.0 filtering for mash-up Web portals that blocks panels and dynamic content per policy settings
- Centralized management via ZyXEL CNM
- ZyXEL Vantage Report helps analyzing Internet access behavior and finding potential risks

Application Benefits

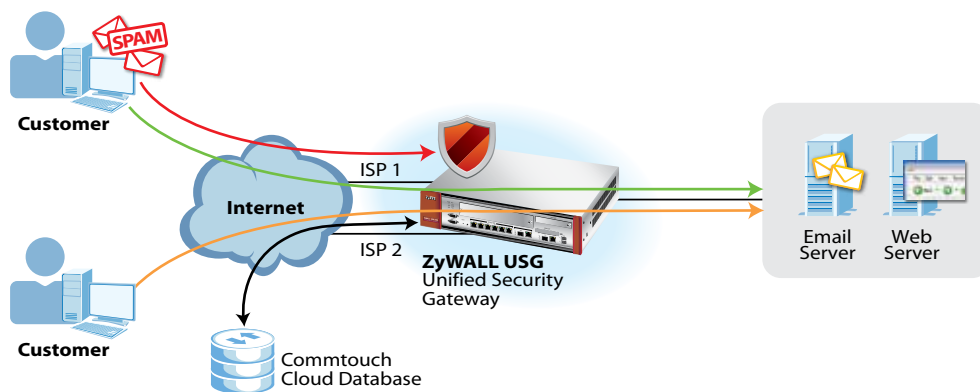
- Malware protection — enabling real-time protection from emerging Web threats including malware and phishing.
- Increased employee productivity — monitoring and blocking suspicious sites to maximize employee productivity
- Bandwidth regulation — identifying sites that consume a significant amount of bandwidth (e.g. movies and music sites)

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 ZyWALL USG Series provides Anti-Spam features to keep spam off your network.



Performance Features

- Anti-Spam technology powered by Commtouch
- Unique RPD technology — block all associated spam messages in real time
- Sender-based IP reputation — removes over 80% of the unwanted mails
- Zero-hour Virus Outbreak Protection — USG blocks or delays suspect messages hours before commercial Anti-Virus signatures become available

Application Benefits

- Reducing waste of necessary system resources
- Saving bandwidth and enhancing performance
- Increasing information security



Products at a Glance



■ Unified Security Gateway for Small Businesses

The ZyWALL USG 20/20W/50/100/200 Series is designed for small business to provide real-time inspection and multi-layer network protection to prevent the network from threats. The USG Series embodies Stateful Packet Inspection (SPI) Firewall, Anti-Virus (AV), Intrusion Detection and Prevention (IDP), Content Filtering, Anti-Spam and VPN (IPSec/SSL/L2TP) features in one box.

Key Features

- Robust security without sacrificing performance
- Comprehensive support to IPv6
- Zero-configuration remote access with Easy VPN
- Support L2TP VPN on mobile device (iPhone and Android phone)
- ICSA Firewall, IPSec certification
- Content filter stops malware and Web threats
- Non-stop Internet access with multiple WAN and 3G backups



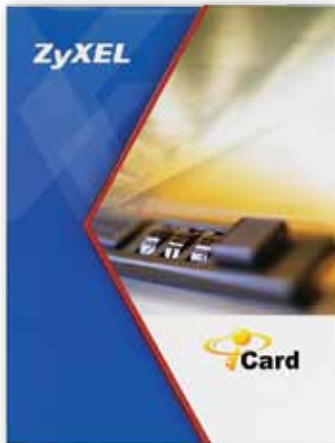
■ Unified Security Gateway for Small and Medium-Sized Business

The ZyWALL USG 300/1000/2000 Series are security platforms that offers ultra-high performance, deep packet inspection and all-in-one multi-threat protection not only to block the latest attack combinations including intrusion attempts, viruses, worms, phishing, spyware, spam and many other malware types effectively, but also to secure remote access among branch offices, partners and customers.



Key Features

- Ultra-high performance and protection
- Comprehensive support to IPv6
- Zero-configuration remote access with Easy VPN
- Support L2TP VPN on mobile device (iPhone and Android phone)
- ICSA Firewall, IPSec certification
- Real-time, dynamic malware protection
- High Availability (HA)



■ Security License and Service

The ZyWALL USG works with comprehensive security licenses and services to guarantee secure corporate network. The ZyWALL Security License services are continuously performed by a 24x7 security update server to automatically deliver updated signature databases to ZyWALL units around the world.

License Category

- Kaspersky & ZyXEL Anti-Virus
- Intrusion Detection and Prevention (IDP)
- Blue Coat & Commtouch Content Filter
- Commtouch Anti-Spam
- SSL VPN
- IPSec VPN Client



■ Vantage Report

The Vantage Report automatically generates clearly laid-out reports of distributed ZyWALLs and graphically portrays Anti-Virus, Anti-Spam and IDP security activities on the ZyWALL UTM devices.

Key Features

- Comprehensive set of graphical reports
- Web-based user interface (browser based application)
- Intuitive design and easy to use
- Automated report scheduling



■ Vantage CNM

The Vantage CNM is a browser-based management tool for service providers and IT staff. Distributed network components can be configured, analyzed and supervised centrally.

Key Features

- Central management
- One-click VPN creation and graphical VPN management
- Mass firewall ACL policy deployment and management
- Bulk firmware upgrade and management

Corporate Headquarters

ZyXEL Communications Corp.

Tel: +886-3-578-3942

Fax: +886-3-578-2439

Email: sales@zyxel.com.tw

<http://www.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

Email: info@zyxel.kz

<http://www.zyxel.kz>

ZyXEL Malaysia

Tel: +603-7960-0088

Fax: +603-7960-8802

Email: sales@zyxel.com.my

<http://www.zyxel.com.my>

ZyXEL Pakistan

Tel: +92 213 4310194-5

Fax: +92 213 4310196

Email: sales@zyxel.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>

■ Europe

ZyXEL Belarus

Tel/Fax: +375 17 334-60-99

Email: info@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 Bulgaria

Tel: +359 2 4443343

Email: info@zyxel.bg

<http://www.zyxel.bg>

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/Fax: +380 44 494-49-31

Email: sales@modem.com.ua

<http://www.ua.zyxel.com>

