

**ZyXEL**

# More than a Firewall!

New Family Members:  
ZyWALL USG 20,  
20W and 50



**ZyWALL USG  
20/20W/50**  
Application Guide

2010

**Big Security for Small Businesses**



## Table of Content

Editorial	4
Scenarios	8
Connecting USG to the Internet	8
Load Balancing and Customised WAN Connections	9
Configure NAT	10
Secure Site-To-Site Connections	11
Secure Client-To-Site Connections	12
Deploying SSL VPN for Teleworkers	13
Priority for VoIP Traffic	14
Priority for a Superior User	15
Control Popular P2P Applications	16
Manage Employee Browsing Behavior	17
Products at a Glance	18



## Editorial

### ***Dear Reseller,***

We are happy to introduce our new Application Guide for ZyWALL security appliances. Our latest Unified Security Gateways 20, 20W (wireless) and 50 address the needs of small businesses with two to ten users and complete the transition from former ZyNOS-based to new ZLD-based security appliances. Being the highlights of the 2010 ZyXEL security product range, the new USGs provide a wealth of security features, and we feel that they deserve a whole new Application Guide.

When I started comparing throughput rates and compiling lengthy feature lists, an important question suddenly crossed my mind. What kind of material do resellers really need? Do they really just need comprehensive technical data to sell our excellent new products? The answer was quite surprising. No, they actually need much more than

that! Well, of course they do need those lists, but in the first place, they need more practical information. As our new USGs address the needs of small companies with few employees and as in those companies, general managers often take on the role of IT administrator, the practical use of a firewall is very important, while technical details are less important. Small companies simply want to know whether our products have what it takes to protect their network against today's network threats, allowing them to go about their business as usual.

These thoughts brought me to the conclusion that I should approach the whole thing not from a security expert point of view, but from the point of view of a small company. After checking all the notes I had made in conversations with small resellers at the Cebit in 2010, where we first



presented our new USG series, I finally found what I needed. A representative of a small chocolate company had asked me many questions, and those were exactly the questions I would ask if I was to run a small business! His focus was of course on how to best go about his daily business of selling chocolate, cookies and candy, rather than on security implementations. Please have a look at the blue boxes for more details on the security challenges of that specific company.

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*

# The Chocolate Factory

Founded in 1970, a small chocolate factory in Western Europe has currently got eleven employees and two branch offices with three more employees each. In addition, there are several remote workers and some freelance employees, such as translators, who occasionally need to access company resources. The company faces a range of challenges we probably can solve with this guide.

**Challenge: Internet downtime causes my company a lot of expense. We really need continuous Internet access!**

*Solution:* Multiple WANs allow your company to stay online. Use redundant Internet connections or 3G as a backup, and you will not suffer from downtime again.

*See more on page 8*

**Challenge: I would like my company to be more cost-effective by using different Internet access providers.**

*Solution:* Use customised WAN connections to use the provider of your choice for the traffic you have at a specific time. The other WAN connection is only used for backup purposes.

*See more on page 9*

**Challenge: My staff and I often have to attend trade fairs. That means we all need to be online and still be protected by excellent security features.**

*Solution:* Use the 3G support of your ZyWALL. With a 3G dongle, you can easily establish a safe Internet connection wherever you are. For suitable dongles, check out the ZyXEL website.

*See more on page 10*

**Challenge: I want my customers to be able to download our brochures and visit our website without provoking a security breach.**

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

**Challenge: Our company has got two branch offices. I would like to securely integrate them into our company network.**

*Solution:* IPsec VPN enables you to establish secure tunnels via Internet. This allows your staff in the branch offices to access the company network the same way as anyone working in the head office. Just install a ZyWALL in each location and establish a secure connection.

*See more on page 11*

**Challenge: Excellent! And what about our sales team, do they need a firewall too? We are looking for an inexpensive solution for them as well.**

*Solution:* With the IPsec client software, you can enable clients to build up a client-to-site connection. The principle is the same as for a site-to-site connection (headquarter/branches), but the software is installed on the computer and therefore easier to handle.

*See more on page 12*

**Challenge: Our company works with several freelancers, who only need very seldom and very limited access to our network. What would you suggest?**

*Solution:* In that case, SSL-VPN is the ideal solution. By simply using their browser, freelancers can easily access the ZyWALL and build up a secure tunnel (which is the same technology as used in online banking). As no software is required, this represents an easy and inexpensive way to access the company network for people who only rarely need the company's resources.

*See more on page 13*

**Challenge: We use VoIP to reduce telephone costs. How can we get excellent voice data quality?**

*Solution:* Bandwidth management enables you to prioritise VoIP or any other traffic to ensure highest quality with neither delay nor jitter. This will prevent less important traffic such as FTP traffic from eating up your bandwidth.

*See more on page 14*

**Challenge: As the boss of the company, I need to have highest bandwidth priority. The same is true for other important managers including my sales team.**

*Solution:* You can use the bandwidth management function to assign a certain bandwidth to each user, so that you and other important managers have absolute priority in the network. You can further limit the number of sessions of other users, avoiding bottlenecks.

*See more on page 15*

**Challenge: I've noticed that more and more of my employees use P2P applications. I need to get in control**

**of this, so that they can focus on their work and I do not have to deal with abusive use of the Internet, which could cost me a lot of money!**

*Solution:* With the "Application control" function, you have granular control of IM and P2P applications down to the user. Allow apps which are necessary for the business, but restrict them to specific users, a defined usage time and a maximum available bandwidth. (IM/P2P requires an IDP service license).

*See more on page 16*

**Challenge: I want my employees to be able to study our competitors' offers, but I need to control their Internet activities in order to prevent private surfing.**

*Solution:* Content filtering offers you a huge number of different categories, ranging from "Pornography" to "Real Estate". Decide which websites your employees are allowed to access and which they are not. Alternatively, you can allow them to only visit the websites you actually want them to access. There are manifold possibilities.

*See more on page 17*

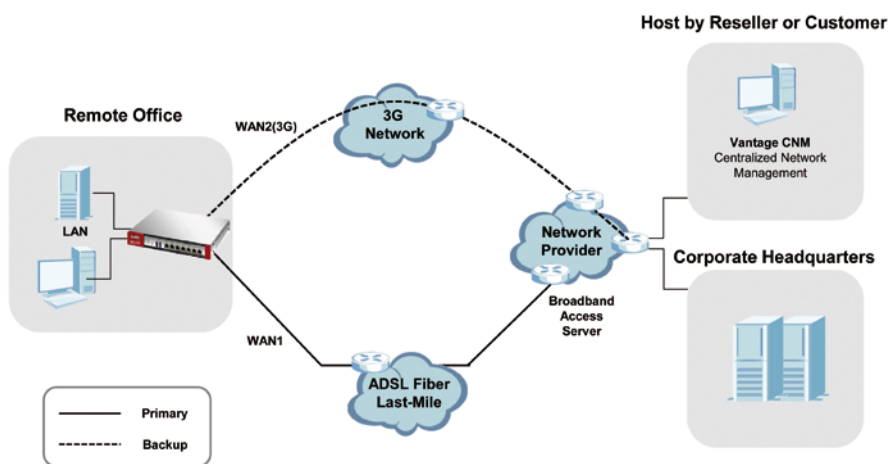
After discussing the requirements with the general manager of the company, the reseller offered him a tailored solution to protect his network from various security threats. Firstly, the general manager decided to go for the USG 50 with two Gigabit WAN ports, 3G for backup purposes and five IPsec VPN connections. Secondly, he decided to use a USG 20 in his branch office. Thirdly, he bought a SSL license to increase his number of SSL VPN tunnels from two to five, to make sure all his freelancers could access the company's resources. Additionally, in order to gain better control of his employees' activities, he purchased a license for content filtering.



## ZyXEL Benefits at a Glance:

- Non Stop Internet access
- Lifetime care - Up-to-date protection while saving your firmware upgrade cost before product's end of life (Available for USG 20/20W/50)
- World's 1st Green Firewall - Up to 80% power consumption reduction with ZyXEL IntelliEnergy Green technology
- ICSA Firewall, IPsec certification
- Free local pre- & post-sales support
- ZyXEL's Partner Program at [www.zyxel.com/europe/partner](http://www.zyxel.com/europe/partner)

# How to Connect Your USG to the Internet



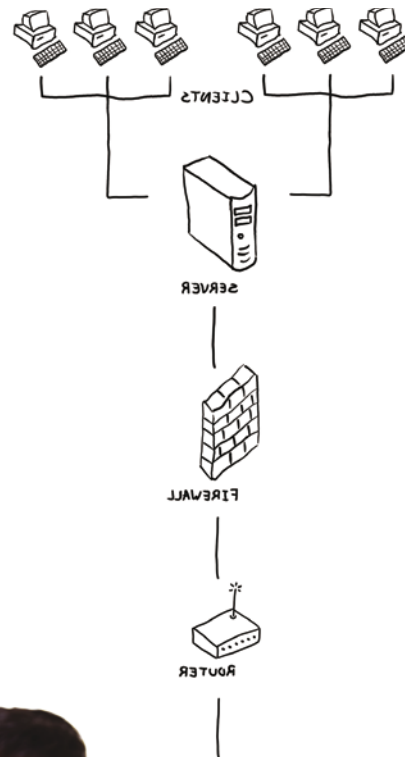
### Benefits for your customer:

- Unlimited Internet access
- 3G as backup or for remote access at fairs etc.
- Centralised management

A WAN (Wide Area Network) covers a broad area, connecting a private network, such as a LAN (Local Area Network), to another network or the Internet. That way, computers in one location can communicate with computers in other locations.

ZyWALL USGs have a multiple WAN feature, which enables users to connect up to two ISPs or networks via Ethernet, PPPoE or 3G connections. Users can either use trunks for WAN traffic load balancing, increasing overall network throughput ("active-active" load sharing mode) or as a backup to enhance network reliability ("active-passive" failover mode).

Load balancing will be described in more detail in Scenario 2. Here, we will show the scenario for unlimited Internet access with PPPoE as primary WAN and 3G backups through USB. This means that the USG will normally use the PPPoE interface for Internet access, switching to the 3G interface when the PPPoE connection fails.



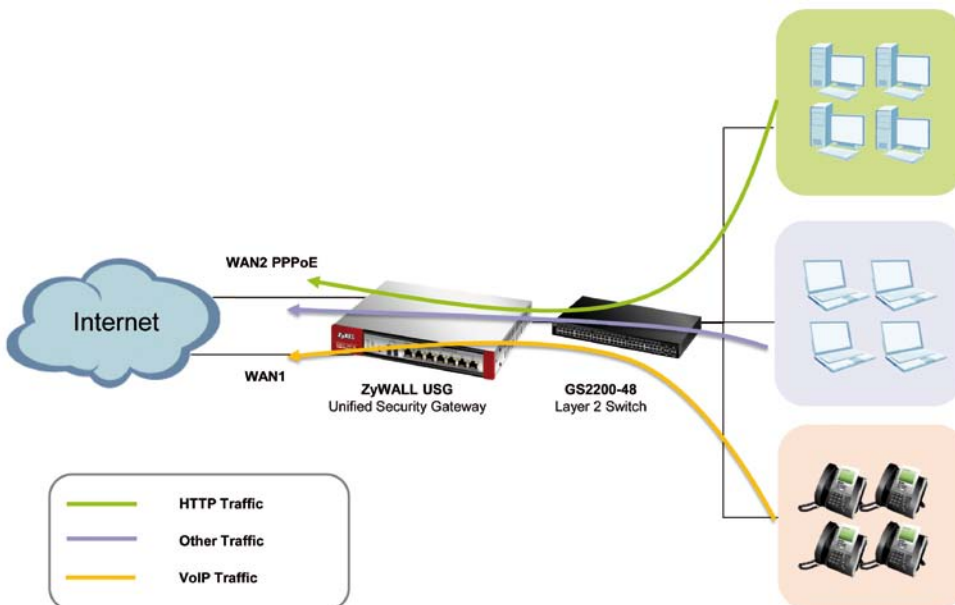
## Scenario 2



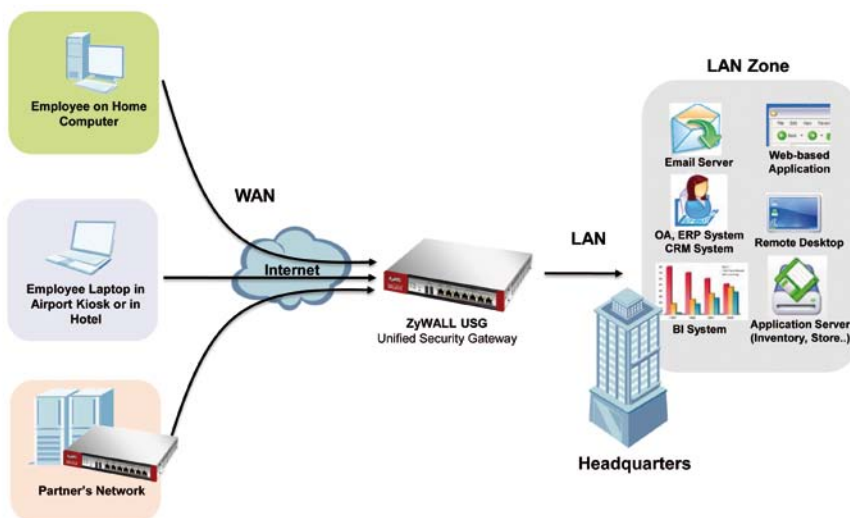
# How to Use Load Balancing and Customised WAN Connections

Our chocolate factory has got two WAN connections to share outbound Internet traffic. WAN1 uses a static IP, while WAN2 uses a PPPoE connection. Since WAN1 ISP is also the company's VoIP provider, the network administrator wants VoIP traffic to be primarily sent out over WAN1. In case WAN1 is down, VoIP traffic can still go out over the WAN2 PPPoE

connection. The administrator also wants HTTP traffic to be sent out primarily over the WAN2 PPPoE connection. In case WAN2 PPPoE is down, LAN users can still surf via WAN1. For all other types of traffic, administrators need the two WAN connections share the outbound traffic load, performing load balancing.



# How to Configure NAT for Internet-Facing Servers



### Benefits for your customer:

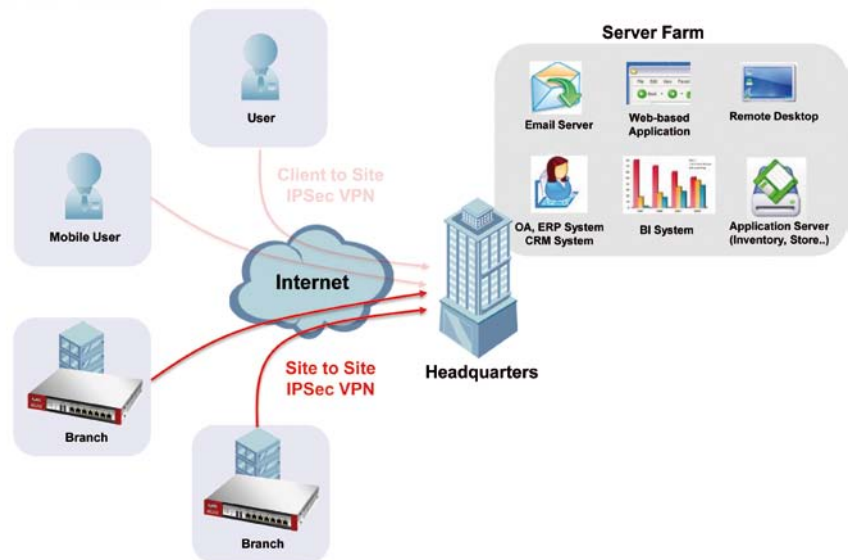
- Reduction of infrastructure costs and company overheads
- Increase in employee productivity and quality of work
- Ability to work in extreme weather conditions
- Flexible working hours for employees
- Reduction of carbon footprint

Placing a server behind a USG, offering maximum network protection while allowing WAN side clients/ servers to access intranet servers, is common practice. A company may for example have a FTP server which needs to be accessed by remote workers over the Internet. To fulfil this requirement,

the administrator can configure a NAT mapping rule, forwarding the traffic from Internet to intranet. That way, telecommuters can remotely access the company's network while avoiding attacks on the server's real IP address.



# How to Secure Site-To-Site Connections Using IPSec VPN



A virtual private network (VPN) provides secure communication between distant sites without the expense of leased site-to-site lines. A secure VPN combines tunnelling, encryption, authentication, access control and auditing to securely transmit data over the Internet or any other insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for the secure transmission of data across a public network 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

and the remote IPSec router will use. In the first phase, an Internet Key Exchange (IKE) SA is established between the ZyWALL and the remote IPSec router. In the second phase, IKE SA is used to securely establish an IPSec SA allowing the ZyWALL and the remote IPSec router to exchange data between computers on the local network and computers on the remote network.

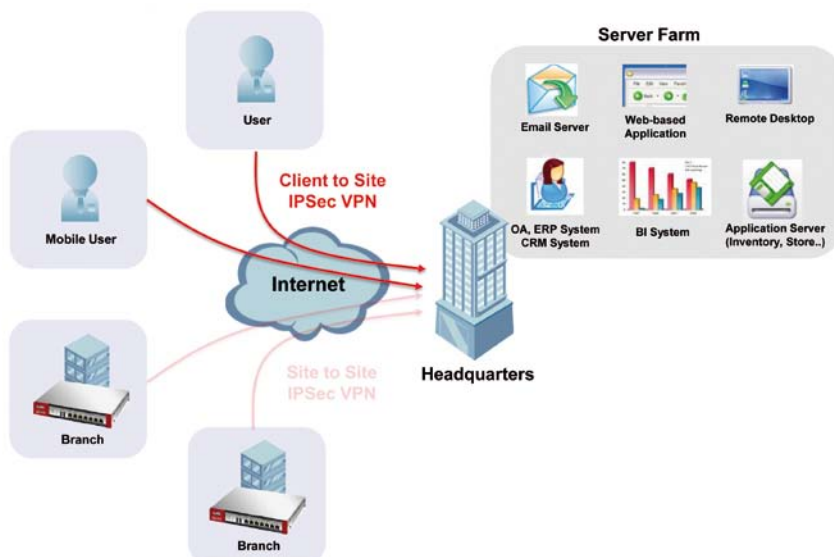
ZyWALL USGs provide secure site-to-site communication between remote locations and corporate resources through the Internet. Using IPSec VPN, companies can secure connections to branch offices, partners and headquarters as illustrated below.



## How to Secure Client-To-Site Connections Using IPSec VPN

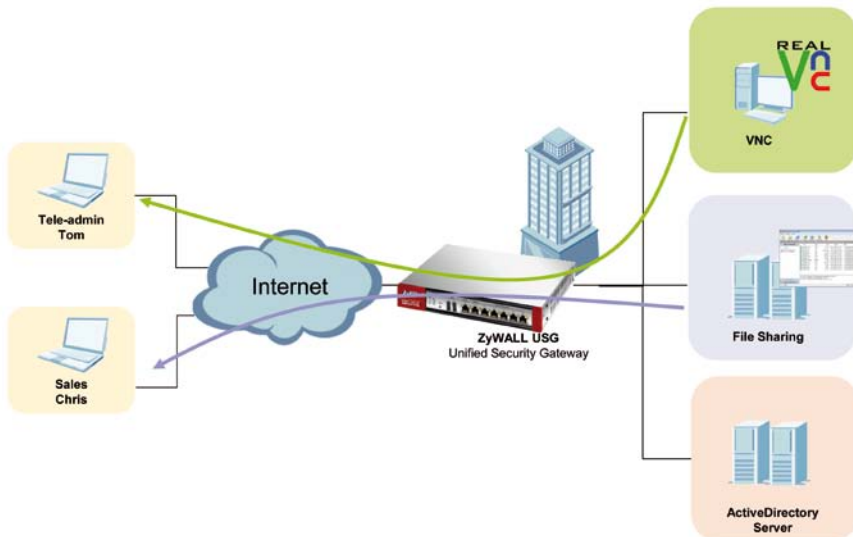
Remote workers and telecommuters can use SSL or IPSec VPN to safely access the company network without having to install VPN software. The ZyWALL USG series provides a flexible and easy way to enable remote workers, vendors and partners to securely access your network resources, improving both security and efficiency.

The ZyWALL USG series is suitable for organisations of any size. Using IPSec VPN, any company can establish secure connections to its branch offices, partners and headquarters.



## Scenario 6

# How to Use SSL VPN to Remotely Access Company Resources



Telecommuters sometimes need to securely access their company's resources. While the establishment of an IPSec tunnel to the company gateway is an option, the Windows VPN client configuration is too complicated. To configure IPSec VPN more easily, the installation of additional IPSec VPN client software is required.

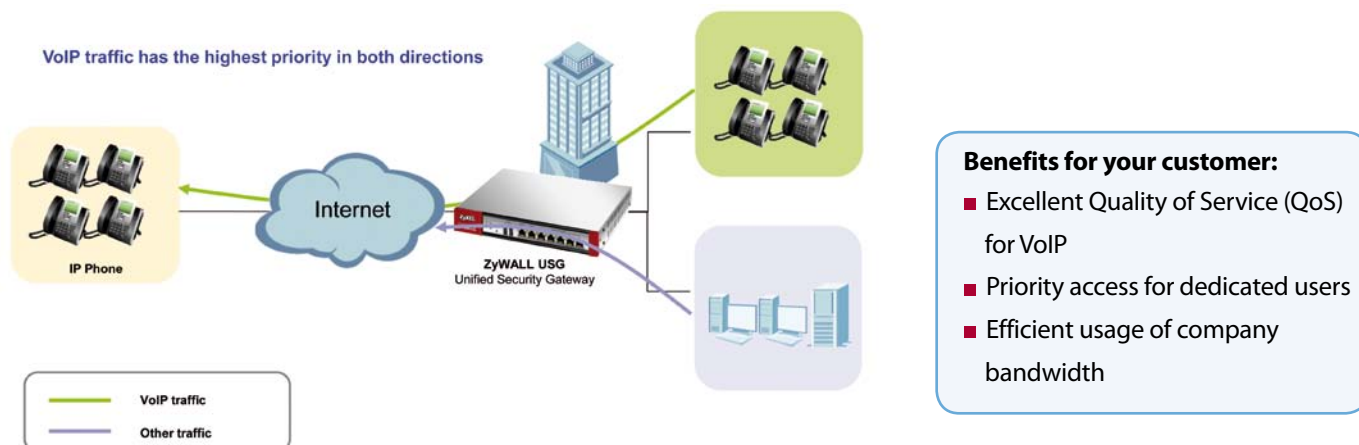
The USG ZyWALL provides a SSL VPN function, enabling telecommuters to easily access company resources via a secure VPN tunnel. All they need on their PC is a browser. Besides, SSL VPN enables network administrator to define individual access rules, allowing for different user profiles with grant users access to different company resources.

That way, a network administrator can set up a SSL VPN rule to allow administrator Tom to remotely control company servers by RDP or VNC through SSL VPN tunnels. He can also set up a SSL VPN rule to allow the sales team to remotely access company file share resources, helping them fulfil their daily tasks.



**Please note:** The USG 20/20W/50 does not support SSL VPN file share and OWA applications so far. If remote clients want to use file share and OWA through SSL VPN, they can use the SSL VPN full tunnel mode (Security Extender) as a workaround.

# How to Prioritising VoIP Traffic



There are various types of traffic in a company network. The company's bandwidth being limited to a certain amount of traffic, some traffic has to be given priority. Otherwise, the excessive use of limited bandwidth may slow down or delay important traffic, such as VoIP. Therefore, and in order to improve productivity, the wise use of bandwidth has become a major concern to network administrators. ZyXEL ZyWALLs provide a Bandwidth Management (BWM) function to effectively manage bandwidth according to flexible criteria. VoIP traffic is prone to delay and jitter. Therefore, VoIP traffic is usually granted highest priority in any company network, being more time-sensitive than other traffic types.





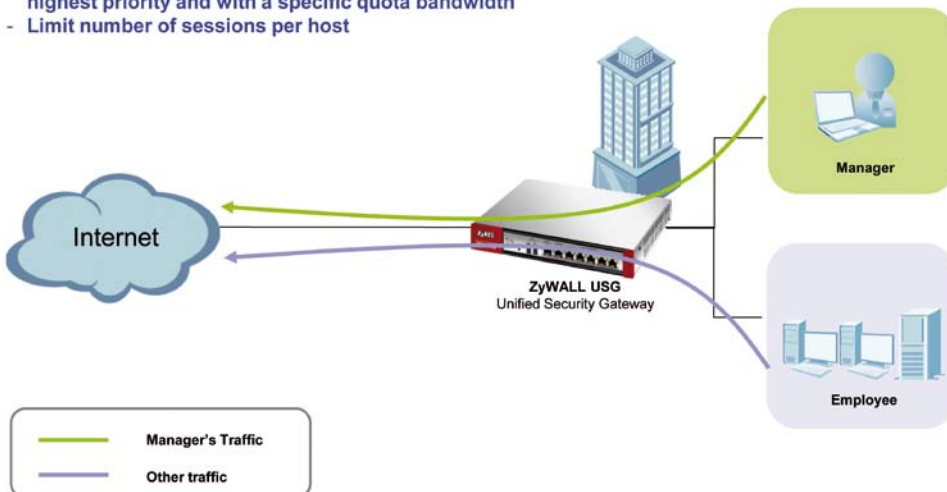
# How to Give Number One Priority to Key User and Control Session per Host

There are users in a company's network that need to be given priority over all other users, as they perform important tasks which make them more strongly depend on a reliable transmission of data. A general manager, for example, needs permanent access to Internet in order to perform his daily tasks. Network administrators should use the bandwidth management function to give the general manager's Internet

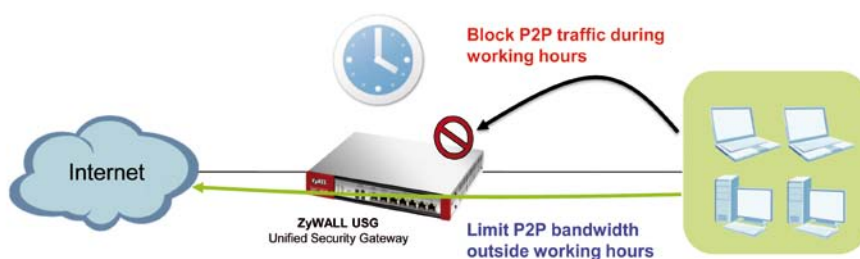
traffic highest priority, reserving a certain bandwidth for that particular user.

Furthermore, network administrators should set up a limit during working hours, confining each user to a certain number of sessions, preventing them from using up too much of the company's bandwidth.

- Guarantee managers' internet surfing traffic has the highest priority and with a specific quota bandwidth
- Limit number of sessions per host



## How to Use Application Patrol for Popular P2P Applications



### Benefits for your customer:

- Saving money by increasing productivity
- Granular control of user's rights
- Reducing dangers due to abusive use of Internet
- Full control of company network

Peer to Peer (P2P) applications require a great number of concurrent sessions and a fast data transmission rate, thereby consuming much of a company's limited bandwidth. This will slow down productive traffic, affecting productivity and decreasing a company profits. The Application Patrol function in ZyWALL USGs can examine passing traffic in real time,

detecting traffic service types and taking action according to the configurations defined in Application Patrol. To improve network productivity and efficiency, network administrators can for instance configure Application Patrol to block P2P traffic during working hours, and limit its speed with bandwidth management outside working hours.

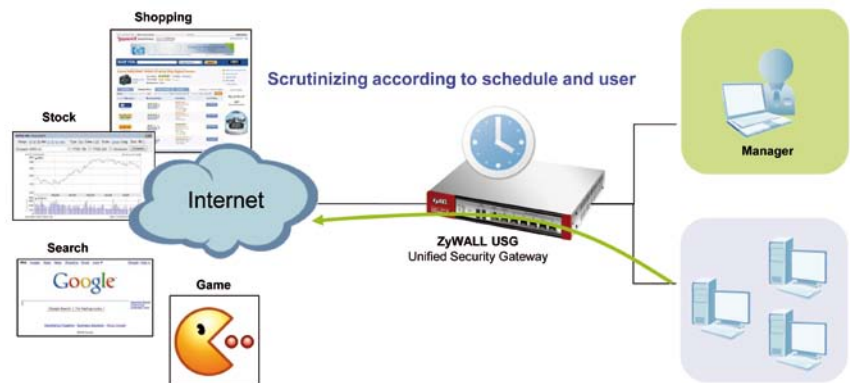


**Please note:** Application Patrol is only supported by USG 50.  
1 year licence available from Q1/2011.



## Scenario 10

# How to Control Employee Use of the Internet with Content Filtering



In order to fulfil their daily tasks, staff need to be able use the Internet as main source of information. However, browsing websites which are not job-related is a waste of human resources as well as a waste of company network resources. In addition, some websites may threaten the company's network, attempting to acquire sensitive information by phishing or accessing the system by introducing malicious codes. Such unsafe websites should be avoided. That means that the network administrator needs to implement policies to avoid this kind of browsing. ZyXEL Content Filtering service, including its Safe Browsing service, is tailored to help network administrators deal with these requirements.

During working hours, employees should concentrate on their work and be prevented from browsing websites that have nothing to do with their work. Nevertheless, managers should be able to access all websites without any restrictions at all times, except for unsafe websites of course. Restrictions for employees can be removed as soon as official working hours are over, giving them access to all websites except for unsafe websites.

## Products at a Glance

### ZyWALL USG 20

- Unified Security Gateway for SB (1~5 PC users)
- All Gigabit Ethernet interface hardware design
- High-performance multi-layer threat protection
- Hybrid VPN (IPSec and SSL) for secure connections
- 3G USB dongle the backup WAN



### ZyWALL USG 20W

- Unified Security Gateway for SB (1~5 PC users)
- All Gigabit Ethernet interface hardware design
- High-performance multi-layer threat protection
- Hybrid VPN (IPSec and SSL) for secure connections
- 3G USB dongle the backup WAN
- 802.11b/g/n wireless Access Point



### ZyWALL USG 50

- Unified Security Gateway for SB (1~10 PC users)
- All Gigabit Ethernet interface hardware design
- High-performance multi-layer threat protection
- Hybrid VPN (IPSec and SSL) for secure connections
- Multiple WAN ports for multiple ISP links and load balancing



Model	ZyWALL USG 20	ZyWALL USG 20W	ZyWALL USG 50
<b>Hardware</b>			
<b>Physical Ports</b>	4 x LAN/DMZ, 1 x WAN (All GbE)	4 x LAN/DMZ, 1 x WAN (All GbE)	4 x LAN/DMZ, 2 x WAN (All GbE)
<b>USB Ports</b>	1	1	2
<b>802.11b/g/n</b>	-	Yes	-
<b>Performance</b>			
<b>Firewall Throughput</b>	100Mbps	100Mbps	100Mbps
<b>UTM Throughput (AV+IDP+Firewall)</b>	-	-	15
<b>Unlimited User Licences</b>	Yes	Yes	Yes
<b>Sessions</b>	6,000	6,000	10,000
<b>Max. Concurrent IPSec VPN Tunnels</b>	2	2	5
<b>Max. Concurrent SSL VPN Users</b>	1	1	5

[www.zyxel.com/usg](http://www.zyxel.com/usg)



UNIFIED SECURITY GATEWAY



TESTIMONIALS

- [Sjors Brul, Managing Director, SBit Hospitality Services](#)
- Ben Frost, Director, Network Needs Ltd
- Dave Brook, Director of Internet Services, iDS
- Russell Carleton, IT Director, Stanley Gibbons

MULTIMEDIA

DEMONSTRATION

PRODUCT SELECTOR



**Sjors Brul, Managing Director, SBit Hospitality Services**

I was impressed with the ZyWALL's high performance while handling anti-virus, intrusion detection and prevention, content filtering, and other services. ZyWALL met and exceeded our expectations in most cases. So ZyWALL USG will also play a critical role on my customers network, treating different segments, like DMZ etc. We stopped selling any other products, Zywall is our Standard now!!

PRODUCTS

- › ZyWALL USG 50
- › ZyWALL USG 20
- › ZyWALL USG 20W



## 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: +86-010-82800646  
Fax: +86-010-82800587  
Email: sales@zyxel.cn  
<http://www.zyxel.cn>

### ZyXEL China (Guangzhou)

Tel: +86-020-87584480  
Fax: +86-020-87576311  
Email: sales@zyxel.cn  
<http://www.zyxel.cn>

### ZyXEL China (Tianjin)

Tel: +86-022-87893801  
Fax: +86-022-87892304  
Email: sales@zyxel.cn  
<http://www.zyxel.cn>

### ZyXEL China (Wuxi)

Tel: +86-510-88080888  
Fax: +86-510-85222670  
Email: info@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 Pvt. Ltd.

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>

## 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  
Fax: +358-9-4780 8448  
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 510  
Email: sales@zyxel.de  
<http://www.zyxel.de>

### ZyXEL Hungary

Tel: +36-1-336-1646  
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 A/S

Tel: +47 23 37 12 00  
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 (Stockholm)

Tel: +46 8 752 9600  
Fax: +46 8 752 9610  
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.Ş.

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>

## The Americas

### ZyXEL Costa Rica

Tel: +506-22017878  
Fax: +506-22015098  
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://www.us.zyxel.com>