

ZyXEL

Plus qu'un pare-feu!

USG 20, 20W et 50 :
Bienvenue dans la
famille des ZyWALL



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

2010 - 2011

Pare-feux performants pour PME



Table des matières

Editorial	4
Scénarios	8
Connecter votre USG à Internet	8
Équilibrage de charge et connexions WAN personnalisées	9
Configuration NAT	10
Connexions site à site sécurisées	11
Connexions client à site sécurisées	12
Accès à distance via VPN SSL	13
Prioriser le trafic VoIP	14
Prioriser les utilisateurs clés et contrôler les sessions	15
Application Patrol pour les applications P2P	16
Filtrage de contenu pour contrôler l'utilisation d'Internet	17
Aperçu des produits de sécurité	18

Editorial

Chers revendeurs,

Nous sommes heureux de vous présenter notre nouveau guide d'application pour les boîtiers de sécurité ZyWALL. Nos toutes nouvelles Unified Security Gateways USG 20, 20W (sans fil) et 50 répondent aux besoins des petites entreprises comptant deux à dix utilisateurs, et terminent la transition entre les anciens boîtiers de sécurité basés sur Zynos et ceux basés sur le nouveau ZLD. Produits phares de la gamme de sécurité ZyXEL 2010, les nouveaux USGs fournissent une richesse de caractéristiques de sécurité et nous pensons qu'ils méritent un nouveau guide d'application.

Lorsque j'ai commencé à comparer les débits et à compiler de longues listes de caractéristiques, je me suis soudain posé une question importante. De quel type de matériel les revendeurs ont-ils réellement besoin ? Ont-ils simplement besoin d'informations techniques complètes afin de vendre nos excellents produits ? La réponse était assez surprenante. Non, en fait ils ont besoin de bien plus que cela ! Bien sûr

ils ont besoin de ces listes, mais en tout premier lieu, ils ont besoin de plus d'informations pratiques. Comme nos derniers USG répondent aux besoins de petites entreprises avec peu d'employés, et que dans ces entreprises les directeurs jouent souvent le rôle d'administrateurs du système informatique, l'utilisation pratique d'un firewall est très importante, tandis que les détails techniques sont moins importants. Les petites entreprises veulent simplement savoir si nos produits fournissent ce qu'il faut pour protéger leur réseau contre les menaces actuelles, leur permettant de s'occuper de leur business habituel.

Ces réflexions m'ont mené à la conclusion que je devais approcher le sujet non du point de vue de l'expert en sécurité, mais du point de vue d'une petite entreprise. Après avoir vérifié toutes les notes que j'ai prises lors de conversations avec des petits revendeurs sur le Cebit 2010, où nous avons présenté notre nouvelle série USG, j'ai enfin trouvé ce que



je cherchais. Le représentant d'une petite usine de chocolat m'a posé de nombreuses questions, et c'était exactement les questions que je poserais si j'avais à diriger une petite entreprise ! Bien sûr, il se concentrait plus sur le meilleur moyen de faire son business quotidien, à savoir vendre des chocolats, biscuits et bonbons, que sur les implémentations de sécurité. Regardez dans les pages suivantes les challenges de cette société en termes de sécurité.

J'espère que ce guide va vous aider à conseiller au mieux vos clients. Notre guide d'application a pour but de vous aider à trouver la bonne solution pour vos clients TPE, en vous aidant à les convaincre tout en leur offrant les meilleures solutions de sécurité sur mesure. Il présente une grande variété de scénarios d'entreprise, fournissant des descriptions détaillées et un diagramme pour chaque scénario. Veuillez aussi vous référer au nouveau Product

Finder, qui vous aide à réaliser des solutions sur mesure, en fonction des besoins spécifiques de vos clients. Nous nous réjouissons de collaborer avec vous !

Meilleures salutations



Thorsten Kurpjuhn
Market Development Manager

t.kurpjuhn@zyxel.de

La fabrique de chocolat

La petite fabrique de chocolat en question a été fondée en 1970. Elle compte à ce jour onze employés et deux filiales avec chacune trois employés. En outre, il y a plusieurs travailleurs distants et quelques employés freelance, tels que des traducteurs, qui ont parfois besoin d'accéder aux ressources de l'entreprise. La société a dû répondre à plusieurs défis en termes de sécurité qui vont être adressés dans ce guide.

Défi : Les interruptions de l'accès à Internet causent à ma société de lourdes dépenses. Nous avons vraiment besoin d'un accès permanent à Internet !

Solution : Les WANs multiples permettent à votre société de rester connectée. Utilisez des connexions Internet redondantes ou le 3G en tant que ligne de secours.

Voir plus de détails page 8

Défi : Je voudrais que ma société soit plus efficace en utilisant différents fournisseurs d'accès à Internet.

Solution : Utilisez des connexions WAN personnalisées pour utiliser le fournisseur de votre choix selon le trafic que vous avez à une heure spécifique. L'autre connexion WAN ne sera utilisée qu'à des fins de ligne de secours.

Voir plus de détails page 9

Défi : Nous participons souvent à des salons où nous devons être connectés tout en restant protégés par d'excellentes caractéristiques de sécurité.

Solution : Utilisez le support 3G de votre ZyWALL. A l'aide de la clé 3G, vous pouvez établir facilement une connexion Internet sécurisée, où que vous soyez. Pour les clés appropriées, veuillez consulter le site Web ZyXEL.

Voir plus de détails page 10

Défi : Je veux que mes clients soient capables de télécharger nos brochures et visiter notre site Web sans provoquer de faille de sécurité.

Solution : Le NAT (Network Address Translation) permet aux clients d'accéder facilement aux serveurs FTP tout en protégeant votre réseau des menaces.

Défi : Notre société a deux filiales. Je voudrais les intégrer au réseau de notre société en toute sécurité.

Solution : Le VPN IPSec vous permet d'établir des tunnels sécurisés via Internet. Ceci permet aux équipes de vos succursales d'accéder au réseau de l'entreprise de la même manière que ceux travaillant au siège social. Installez simplement un ZyWALL sur chaque site.

Voir plus de détails page 11

Défi : Excellent ! Et nos équipes commerciales, ont-elles aussi besoin d'un pare-feu ?

Solution : Avec le logiciel client IPSec, vous permettez à des clients d'établir une connexion client-à-site. Le principe est le même que pour une connexion site-à-site (siège social/filiales), mais le logiciel est installé sur l'ordinateur et est plus facile à manipuler.

Voir plus de détails page 12

Défi : Notre société travaille avec différents employés freelance qui n'ont besoin d'accéder à notre réseau que très rarement et de manière très limitée.

Solution : Dans ce cas, le VPN SSL est la solution idéale. En utilisant simplement leur navigateur Web, ils peuvent facilement accéder au ZyWALL et établir un tunnel sécurisé (il s'agit de la même technologie que celle utilisée pour les banques en ligne). Comme il n'y a pas besoin de logiciel, cela représente un moyen simple et pas cher d'accéder au réseau de l'entreprise pour des personnes qui n'ont que rarement besoin des ressources de l'entreprise.

Voir plus de détails page 13

Défi : Nous utilisons la VoIP: comment pouvons-nous obtenir une excellente qualité voix-données ?

Solution : La gestion de la bande passante vous permet de prioriser le trafic important, afin d'assurer la plus haute qualité de la VoIP sans aucun délai. Ceci évite que du trafic moins important ne mange votre bande passante.

Voir plus de détails page 14

Défi : En tant que directeur de la société, j'ai besoin de la plus grande priorité en termes de bande passante.

Solution : Vous pouvez utiliser la fonction de gestion de la bande passante pour allouer une certaine bande passante à chaque utilisateur, de manière à ce que vous ou d'autres managers importants puissiez avoir la priorité absolue sur le réseau. En outre, vous pouvez limiter le nombre de sessions pour d'autres utilisateurs, ce qui évite les goulets d'étranglement.

Voir plus de détails page 15

Défi : J'ai remarqué que de plus en plus de mes employés utilisent des applications P2P. J'ai besoin de pouvoir

contrôler cela, de manière à ce qu'ils se concentrent sur leur travail et à ce que je n'aie pas à faire face à une utilisation abusive d'Internet.

Solution : Avec la fonction « Application control », vous avez un contrôle granulaire des applications IM et P2P selon l'utilisateur. Autorisez des applications nécessaires à l'entreprise, mais limitez-les à des utilisateurs spécifiques, à un temps d'usage défini et une bande passante disponible maximale (IM/P2P nécessite une licence de service IDP).

Voir plus de détails page 16

Défi : Je veux que mes salariés soient capables d'étudier les offres des concurrents mais j'aimerais bien éviter la navigation à titre personnel ...

Solution : Le filtrage de contenu vous offre un énorme nombre de catégories différentes, de « Pornographie » à « Immobilier ». Décidez des sites sur lesquels vos employés sont autorisés ou pas à surfer. Il existe une multitude de possibilités. Vous pouvez par exemple les autoriser à visiter uniquement les sites que vous voulez effectivement qu'ils consultent.

Voir plus de détails page 17

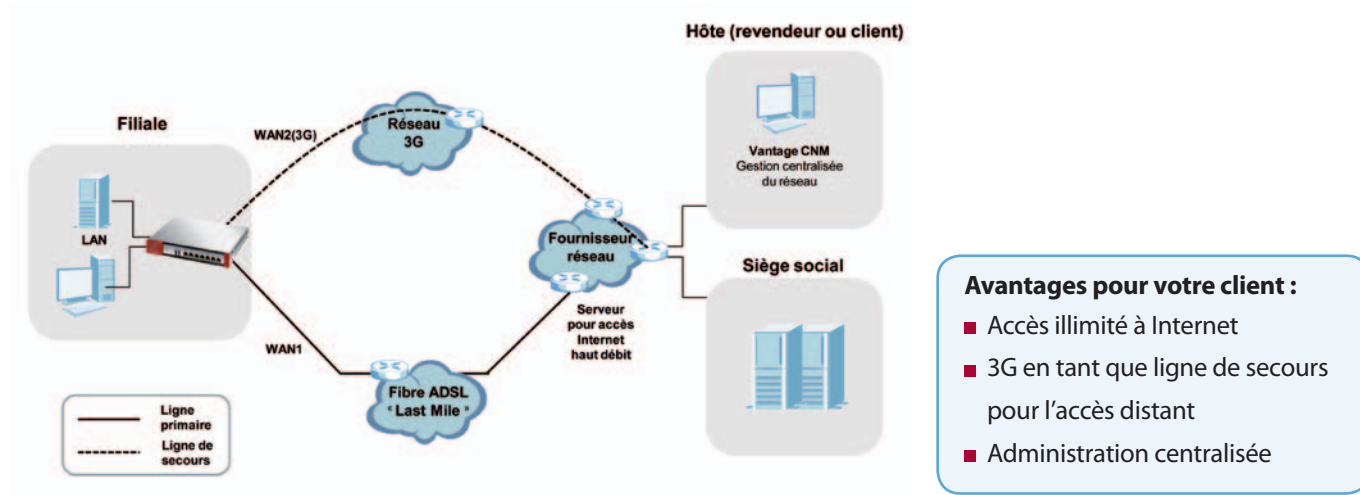
Après avoir discuté les exigences avec le directeur général de la société, le revendeur lui a proposé une solution sur mesure. Tout d'abord, le directeur général a décidé de prendre l'USG 50 avec deux ports WAN Gigabit, le 3G pour des raisons de ligne de secours et cinq connexions VPN IPsec. Deuxièmement, il a décidé d'utiliser un USG 20 dans chaque filiale. Ensuite, il a acheté une licence SSL pour augmenter son nombre de tunnels SSL de deux à cinq, afin de garantir que tous ses freelances puissent accéder aux ressources de l'entreprise. En plus, afin de mieux contrôler les activités de ses employés, il a acheté une licence pour le filtrage du contenu.



Les avantages ZyXEL en un coup d'œil :

- Accès Internet illimité
- Services à vie : mises à jour de firmware gratuites jusqu'à la fin de vie du produit, garantissant une protection complète contre les dernières menaces de sécurité, tout en réduisant considérablement les coûts TOC (disponible pour USG 20, 20W et 50)
- Le premier pare-feu vert au monde : réduction de la consommation énergétique jusqu'à 80% grâce à la technologie ZyXEL IntelliEnergy Green Technology
- Pare-feu ICSA, certification IPsec
- Support avant et après-vente local gratuit
- Partenaires puissants : programme partenaire ZyXEL sur www.zyxel.com/europe/partner

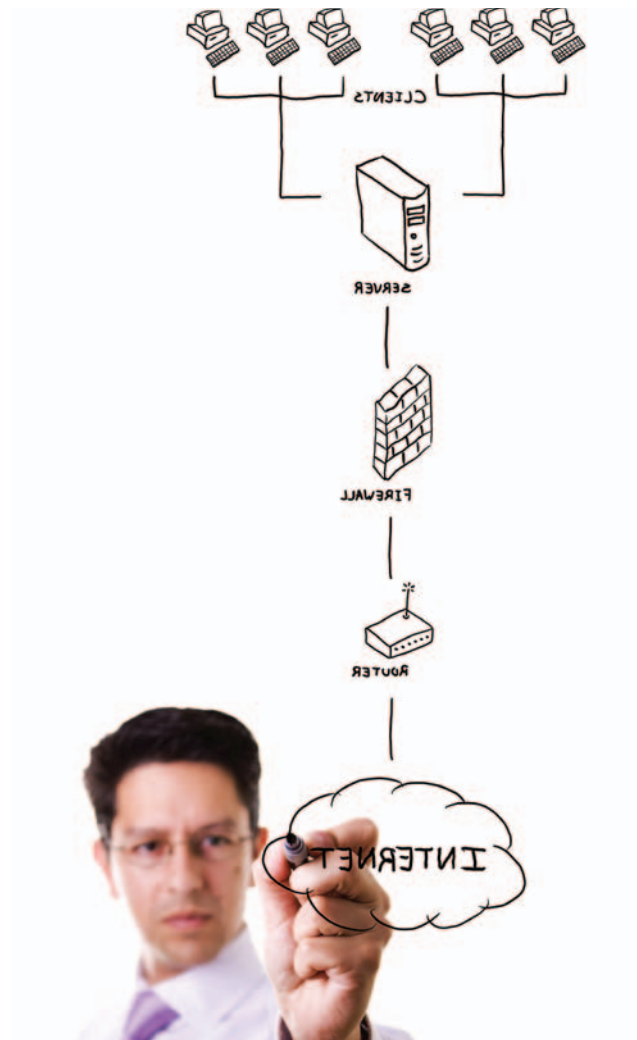
Connecter votre USG à Internet



Un WAN (Wide Area Network) couvre un large secteur, connectant un réseau privé tel qu'un LAN (Local Area Network) à un autre réseau ou à Internet. De cette manière, les ordinateurs sur un site peuvent communiquer avec les ordinateurs sur d'autres sites.

Les ZyWALL USG ont la caractéristique multiple WAN, qui permet aux utilisateurs d'accéder aux deux ISPs ou aux réseaux par le biais de connexions Ethernet, PPPoE ou 3G. Les utilisateurs peuvent utiliser les trunks soit pour l'équilibrage de charge du trafic WAN afin d'augmenter le débit global du réseau (mode répartition de charge « actif-actif »), soit en tant que ligne de secours afin d'améliorer la fiabilité du réseau (mode ligne de secours « actif-passif »).

L'équilibrage de charge sera décrit plus en détail dans le Scénario 2. Ici, nous allons montrer le scénario pour l'accès illimité à Internet avec le PPPoE en tant que WAN primaire et la ligne de secours 3G via USB. Cela signifie que l'USG utilisera normalement l'interface PPPoE pour l'accès à Internet, et basculera vers l'interface 3G si la connexion PPPoE tombe.

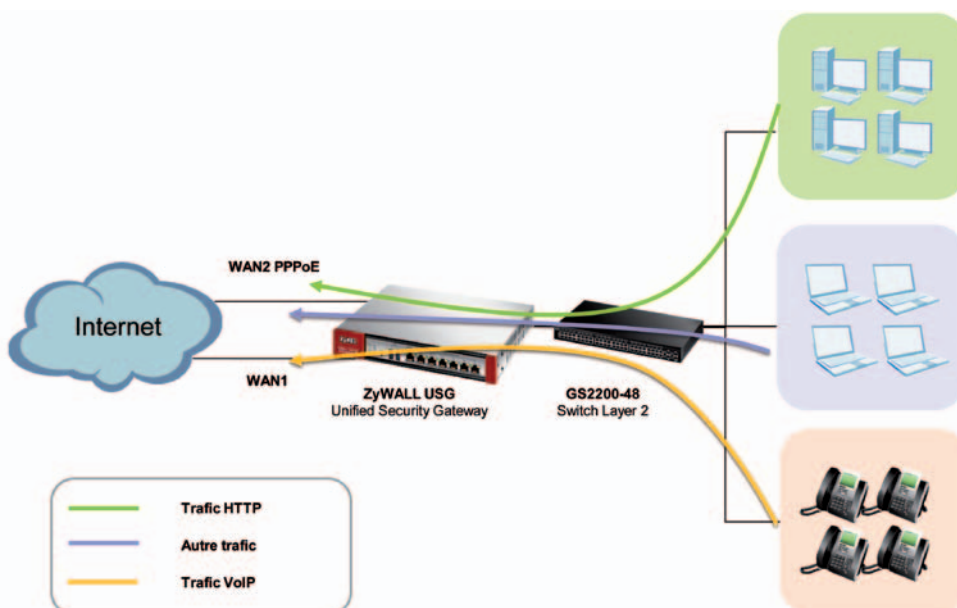




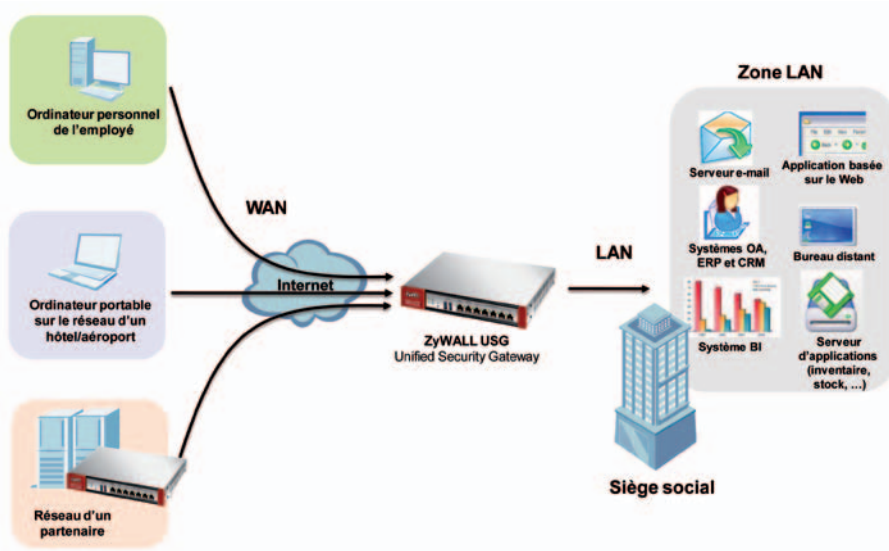
Equilibrage de charge et connexions WAN personnalisées

La société en question a deux connexions WAN pour partager le trafic Internet sortant. Le WAN1 utilise une IP statique, tandis que le WAN2 utilise une connexion PPPoE. Comme l'ISP du WAN1 est également le fournisseur VoIP de la société, l'administrateur du réseau souhaite que le trafic soit envoyé prioritairement par le biais du WAN1. Si le WAN1 tombe, le trafic VoIP peut continuer par le biais de la connexion

PPPoE du WAN2. L'administrateur veut également que le trafic http soit envoyé prioritairement par le biais de la connexion PPPoE du WAN2. Si le PPPoE du WAN2 tombe, les utilisateurs du LAN peuvent continuer à surfer par le biais du WAN1. Pour tous les types de trafic, les administrateurs ont besoin que les deux connexions WAN se partagent la charge du trafic sortant, effectuant l'équilibrage de charge.



Configuration NAT pour les serveurs orientés vers Internet



Avantages pour votre client :

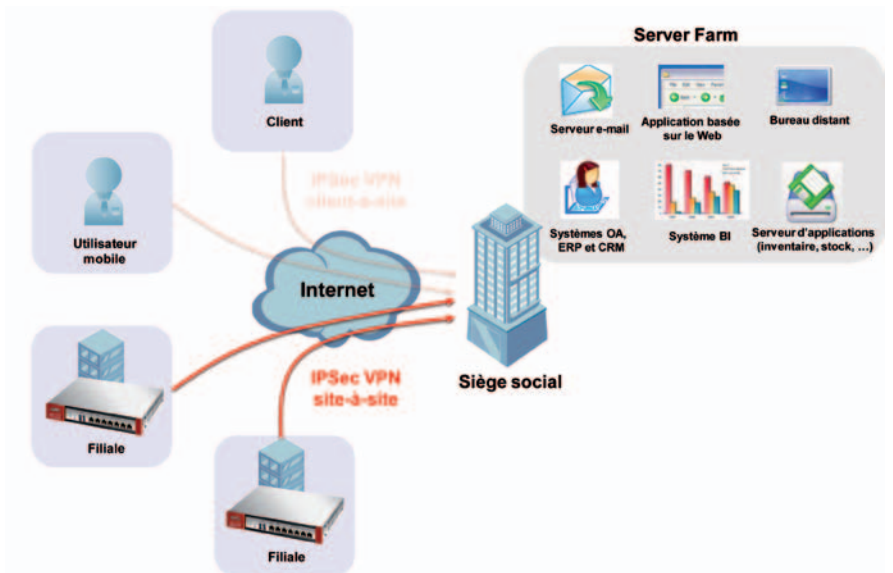
- Réduction des coûts d'infrastructure / des frais généraux
- Augmentation de la productivité des employés & qualité du travail
- Utilisation dans des conditions météorologiques extrêmes
- Horaires de travail flexible
- Réduction de l'empreinte carbone

Le fait de placer un serveur derrière un USG, offrant une protection maximale du réseau tout en permettant aux clients/serveurs du côté WAN d'accéder aux serveurs intranet, est une pratique courante. Une société peut avoir par exemple un serveur FTP auquel les travailleurs distants doivent pouvoir accéder par le biais d'Internet. Afin de satisfaire à cette

exigence, l'administrateur peut configurer une règle NAT, transférant le trafic de l'Internet vers l'intranet. De cette manière, les télétravailleurs peuvent accéder à distance au réseau de l'entreprise, tout en évitant les attaques sur la propre adresse IP du serveur.



Connexions site à site sécurisées en utilisant le VPN IPSec



Un réseau privé virtuel (VPN) fournit une communication sécurisée entre des sites distants, sans avoir à utiliser des lignes spécialisées site à site. Un VPN sécurisé combine le tunnel, le chiffrement, l'authentification, le contrôle d'accès et l'audit, afin de transmettre les données en toute sécurité par le biais d'Internet ou de tout autre réseau non sécurisé utilisant la communication TCP/IP.

L'Internet Protocol Security (IPSec) est un VPN basé sur des standards, qui offre des solutions flexibles pour la transmission sécurisée de données par le biais du réseau public comme Internet. Un tunnel VPN IPSec est habituellement établi en deux phases. Lors de chaque phase, une association de sécurité (SA) est établie. Une SA est une sorte d'agrément indiquant les paramètres de sécurité que le ZyWALL et le

routeur IPSec distant vont utiliser. Dans la première phase, une SA Internet Key Exchange (IKE) est établie entre le ZyWALL et le routeur IPSec distant. Dans la seconde phase, la SA IKE est utilisée pour établir une SA IPSec qui permet au ZyWALL et au routeur IPSec distant d'échanger des données entre les ordinateurs sur le réseau local et les ordinateurs sur le réseau distant.

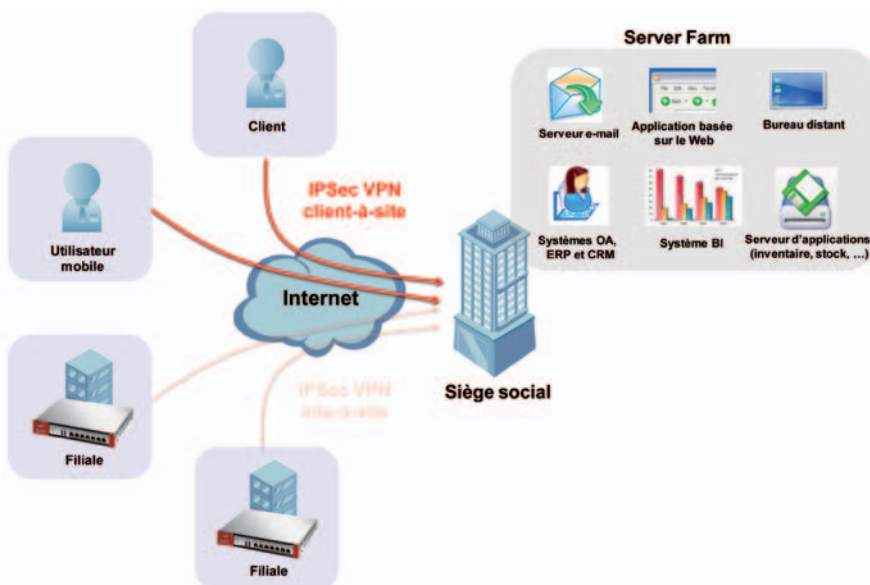
Les ZyWALL USG fournissent une communication site à site sécurisée entre des sites distants et les ressources de l'entreprise par le biais d'Internet. En utilisant le VPN IPSec, les entreprises peuvent sécuriser les connexions vers les filiales, partenaires et sièges sociaux comme illustré ci-dessus.



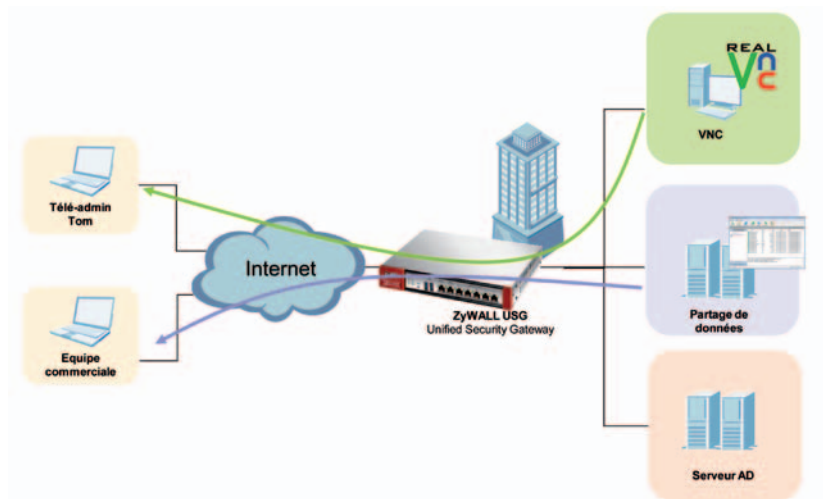
Connexions sécurisées client à site en utilisant le VPN IPSec

Les travailleurs mobiles et télétravailleurs peuvent utiliser le VPN SSL ou IPSec pour accéder en toute sécurité au réseau de l'entreprise sans avoir à installer de logiciel VPN. La série ZyWALL USG fournit une manière flexible et facile de permettre aux travailleurs mobiles, commerciaux et partenaires, d'accéder aux ressources du réseau, améliorant

aussi bien la sécurité que l'efficacité. La série ZyWALL USG est adaptée aux organisations de toute taille. En utilisant le VPN IPSec, n'importe quelle entreprise peut établir des connexions sécurisées vers ses filiales, partenaires et sièges sociaux.



VPN SSL pour accéder à distance aux ressources de l'entreprise



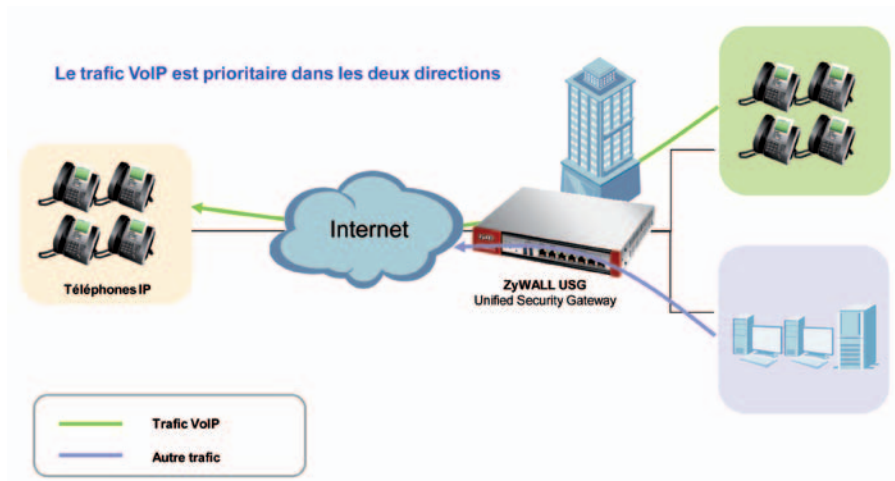
Les télétravailleurs ont souvent besoin d'accéder en sécurité aux ressources de leur entreprise. Alors que l'établissement d'un tunnel IPSec vers la passerelle de l'entreprise est une option, la configuration du client VPN Windows est trop compliquée. Pour configurer plus simplement le VPN IPSec, il est nécessaire d'installer un logiciel client VPN IPSec supplémentaire. Le ZyWALL USG fournit une fonction VPN SSL qui permet aux télétravailleurs d'accéder facilement aux ressources de l'entreprise par le biais d'un tunnel VPN. Ils ont simplement besoin d'un navigateur Web sur leur ordinateur. En outre, le VPN SSL permet à l'administrateur du réseau de définir des règles d'accès personnalisées, permettant d'établir des profils d'utilisateurs différents, ce qui garantit l'accès des utilisateurs à différentes ressources de l'entreprise.

De cette manière, un administrateur réseau peut paramétrer une règle VPN SSL pour autoriser l'administrateur Tom à contrôler à distance les serveurs de l'entreprise par RDP ou VNC à travers des tunnels VPN SSL. Il peut également paramétrer une règle VPN SSL pour autoriser l'équipe commerciale à accéder à distance aux ressources de partage de données de l'entreprise, les permettant de réaliser leurs tâches quotidiennes.



Veillez noter : A ce jour, l'USG 50 ne supporte pas le partage de données VPN SSL et les applications OWA. Si des clients distants veulent utiliser le partage de données et l'OWA par le biais d'un VPN SSL, ils ont la solution d'utiliser le mode VPN SSL full tunnel (Security Extender).

Prioriser le trafic VoIP



Avantages pour votre client :

- Excellente qualité de service (QoS) pour la VoIP
- Accès prioritaire pour des utilisateurs dédiés
- Usage efficace de bande passante

Il existe différents types de trafic sur un réseau d'entreprise. La bande passante de l'entreprise étant limitée à une certaine quantité de trafic, il est nécessaire de donner une priorité à une partie du trafic. Sinon, l'utilisation excessive de la bande passante limitée peut réduire ou retarder le trafic important tel que la VoIP. Ainsi, dans le but d'améliorer la productivité, l'utilisation judicieuse de la bande passante est devenue une préoccupation majeure des administrateurs de réseaux. Les ZyWALL ZyXEL supportent la fonction d'administration de la bande passante (Bandwidth Management, BWM), afin de gérer efficacement la bande passante en fonction de critères flexibles.

Etant plus sensible en temps que les autres types de trafic, le trafic VoIP est sujet au délai et la gigue. C'est pourquoi le trafic VoIP reçoit habituellement la plus haute priorité sur n'importe quel réseau d'entreprise.



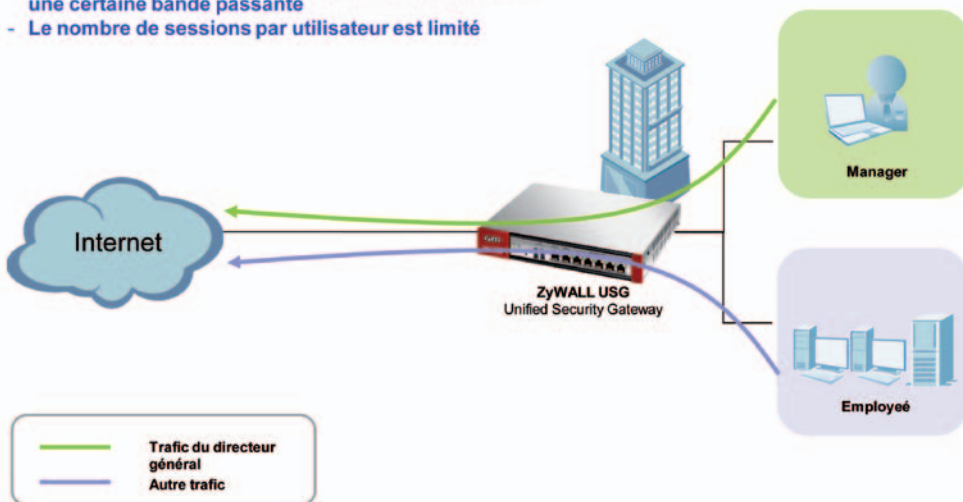


Donner la priorité numéro un aux utilisateurs clés et contrôler les sessions

Sur le réseau d'une entreprise, il est nécessaire de donner la priorité à certains utilisateurs plus qu'à d'autres, parce qu'ils ont des tâches importantes qui les rendent plus dépendants d'une transmission de données fiable. Par exemple, un directeur général a besoin d'un accès Internet permanent afin de réaliser ses tâches quotidiennes. Les administrateurs du réseau devraient utiliser la fonction de gestion de la

bande passante afin de donner la plus haute priorité au trafic Internet du directeur général, réservant une certaine bande passante pour cet utilisateur particulier. En outre, les administrateurs du réseau devraient paramétrer une limite pendant les heures de travail, limitant chaque utilisateur à un certain nombre de sessions, les empêchant d'utiliser trop de bande passante de l'entreprise.

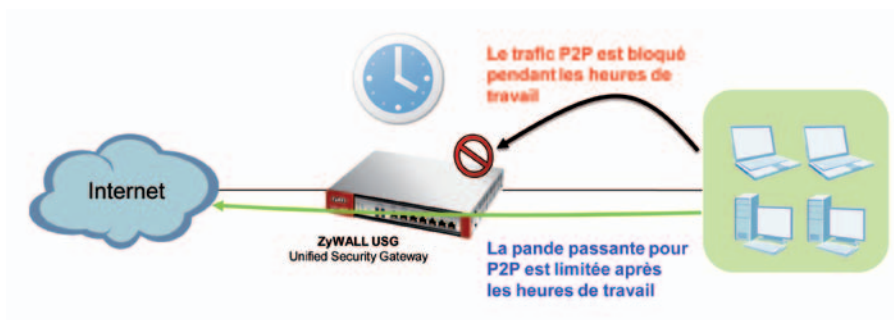
- Le trafic des managers reçoit la plus haute priorité et une certaine bande passante
- Le nombre de sessions par utilisateur est limité



Application Patrol pour les applications P2P populaires

Avantages pour votre client :

- Economies par l'augmentation de la productivité
- Contrôle granulaire des droits d'utilisateurs
- Réduction des dangers résultant d'une utilisation abusive d'Internet
- Contrôle global du réseau de l'entreprise



Les applications PeertoPeer (P2P) nécessitent un grand nombre de sessions concurrentes et un haut débit de transmission, consommant ainsi une grande partie de la bande passante de l'entreprise. Ceci va réduire le trafic productif, ayant une incidence sur la productivité et réduisant les bénéfices de l'entreprise. La fonction Application Patrol intégrée dans les ZyWALL USG peut examiner le trafic passant en temps réel,

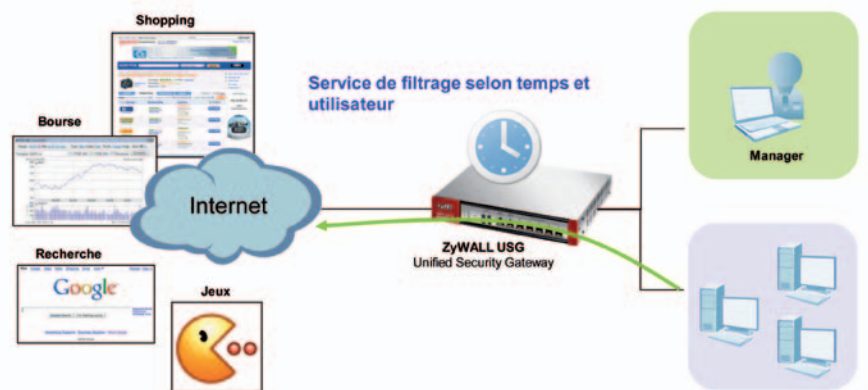
détectant les types de services de trafic et agissant selon les configurations définies dans l'Application Patrol. Afin d'améliorer la productivité et l'efficacité du réseau, les administrateurs du réseau peuvent par exemple configurer l'Application Patrol pour bloquer le trafic P2P pendant les heures de travail et limiter sa vitesse avec la gestion de la bande passante en dehors des heures de travail.



Veillez noter : L'Application Patrol n'est supporté que par l'USG 50. Licence d'un an disponible dès Q1/2011.



Filtrage de contenu pour contrôler l'utilisation d'Internet par les employés



Afin de réaliser leurs tâches quotidiennes, les employés doivent être capables d'utiliser Internet comme source principale d'information. Cependant, la navigation sur des sites web qui n'ont pas de relation avec le travail sont une perte de ressources humaines tout comme une perte des ressources du réseau de l'entreprise. En outre, certains sites Web peuvent menacer le réseau de l'entreprise, essayant d'obtenir des informations sensibles par le biais du phishing ou de l'accès au système, en introduisant des codes malveillants. De tels sites web dangereux doivent être évités. Cela signifie que l'administrateur du réseau a besoin d'implémenter des règles pour éviter ce type de navigation. Le service de filtrage de contenu de ZyXEL, incluant son service Safe Browsing, est

adapté pour aider les administrateurs de réseau à répondre à ce type d'exigences.

Pendant les heures de travail, les employés doivent se concentrer sur leur travail et éviter de naviguer sur des sites Web qui n'ont rien à voir avec leur travail. Néanmoins, les directeurs doivent pouvoir accéder à tous les sites Web sans aucune restriction et à tout moment, sauf pour les sites Web dangereux bien sûr. Les restrictions pour les employés peuvent être levées après les heures de travail, leur donnant l'accès à tous les sites Web, sauf aux sites dangereux.

Aperçu des produits de sécurité

ZyWALL USG 20

- Unified Security Gateway pour petites entreprises (1–5 utilisateurs)
- Tous avec interface Gigabit-Ethernet
- Puissante protection étendue
- VPN hybride (IPSec et SSL) pour des connexions sécurisées
- Dongle 3G USB en tant que ligne WAN de secours



ZyWALL USG 20W

- Unified Security Gateway pour petites entreprises (1–5 utilisateurs)
- Tous avec interface Gigabit-Ethernet
- Performante protection multi-layer
- VPN hybride (IPSec et SSL) pour des connexions sécurisées
- Dongle 3G USB en tant que ligne WAN de secours
- Point d'accès sans fil 802.11b/g/n



ZyWALL USG 50

- Unified Security Gateway pour petites entreprises (1–10 utilisateurs)
- Tous avec interface Gigabit-Ethernet
- Performante protection multi-layer
- VPN hybride (IPSec et SSL) pour des connexions sécurisées
- Ports WAN multiples pour des liens ISP multiples et répartition de charge



Modèle	ZyWALL USG 20	ZyWALL USG 20W	ZyWALL USG 50
Matériel			
Ports physiques	4 x LAN/DMZ, 1 x WAN (tous GbE)	4 x LAN/DMZ, 1 x WAN (tous GbE)	4 x LAN/DMZ, 2 x WAN (tous GbE)
Ports USB	1	1	2
802.11b/g/n	-	Yes	-
Performance			
Débit pare-feu	100 Mbps	100 Mbps	100 Mbps
Débit UTM (AV+IDP+pare-feu)	-	-	15
Licences utilisateurs illimitées	Oui	Oui	Oui
Sessions	6 000	6 000	10 000
Tunnels VPN IPSec simultanés max.	2	2	5
Utilisateurs VPN SSL simultanés max.	1	1	5

www.zyxel.com/usg



Big Security for Small Businesses

ZyWALL USG 50, 20 and 20W

UNIFIED SECURITY GATEWAY



TESTIMONIALS

MULTIMEDIA

DEMONSTRATION

PRODUCT SELECTOR

PRODUCTS

[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



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!!

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

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

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

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

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

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

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

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

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

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>

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: +36-1-336-1646
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
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
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.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>