



ZyXEL ZyWALL USG – Sécurité de dernière génération



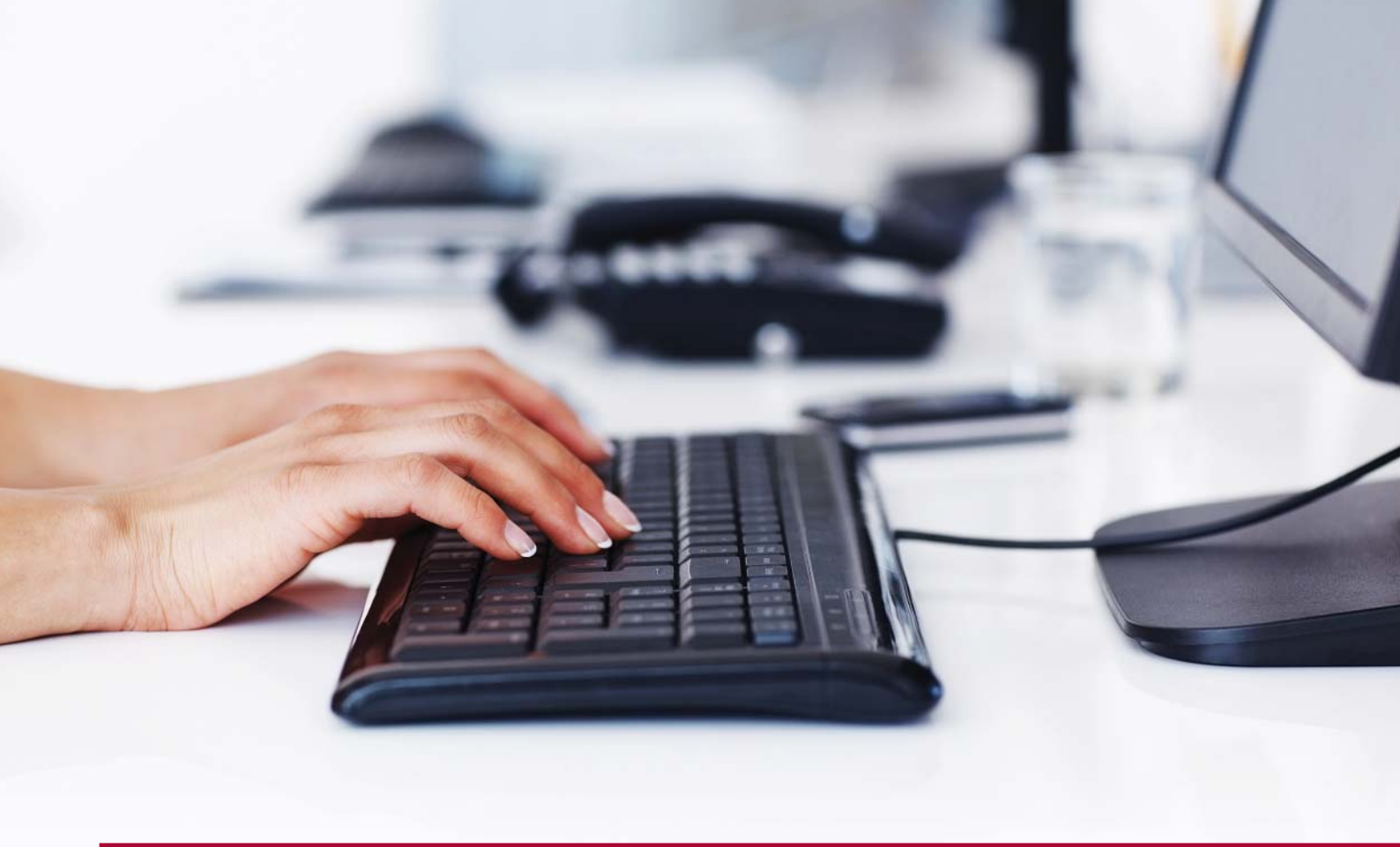
ZyWALL USG Application Guide

- Solutions évolutives
- Services UTM complets
- Simplicité d'installation et de gestion









Sommaire

Préface	6
Cas client : une chaîne de supermarchés	8
Exemples d'applications	10
Connexion sans interruptions grâce aux fonctions backup	10
Connexions Internet performantes	11
Compatibilité et migration IPv6 en toute simplicité	12
Sécurité maximale depuis un serveur	13
Interconnexion sécurisée entre deux sites	14
Connexion sécurisée pour les utilisateurs nomades	15
Accès à distance sur le Web avec règles individuelles	16
Accès à distance avec appareils mobiles et smartphones	17
Gestion de la bande passante et des applications sensibles	18
Optimisation de la rentabilité et productivité des utilisateurs	19
Filtrage de contenu et protection contre les malwares	20
Anti-spam pour une meilleure protection des données confidentielles	21
Aperçu des produits	22

Préface

Cher client,

Il y a maintenant plus d'un an que nous vous avons présenté les nouveaux ZyWALL USG20/20W/50 venant compléter la gamme de sécurité ZyWALL USG de ZyXEL. Depuis, nous avons vendu plus de 20 000 pièces de ces nouveaux produits entrée de gamme et les ventes ne cessent d'augmenter chaque mois.

De plus, le passage de l'ancienne plate-forme ZyNOS à la plate-forme ZLD s'est révélé être un vrai succès. Le nouveau firmware ZLD 3.0 a également été le fruit d'un long travail tout au long de l'année 2011 où nous avons su analyser et identifier toutes les menaces et autres logiciels malveillants. Je ne peux que féliciter notre équipe de R & D pour ce résultat concluant. La protection contre les malwares, l'une des principales menaces dans le domaine de la sécurité d'aujourd'hui, a été considérablement améliorée grâce à l'ajout de nouveaux services dans les USG. En partenariat avec Commtouch, l'un des principaux fournisseurs de solutions de sécurité, nous avons ajouté un des services les plus avancés en termes d'anti-spam sur nos produits sécurité ZyWALL USG.

Plutôt que d'évaluer le contenu des messages, le service anti-spam de Commtouch analyse des milliards d'e-mails en temps réel, identifie et prémunit votre système contre

les spams. L'autre service complémentaire proposé par Commtouch est le filtrage de contenu. Ici encore, nous nous appuyons sur une technologie de pointe et éprouvée pour que vous puissiez disposer d'une solution performante et hautement sécurisée.

Lorsque nous avons conçu le premier guide solution sur les USG en 2010, nous souhaitions l'orienter à destination des revendeurs de petites et moyennes entreprises. Cet objectif n'a pas changé. Des milliers de ces revendeurs nous ont permis de faire de ces produits un succès et grâce à leurs expériences, nous sommes persuadés que ce guide leur a été d'un grand soutien.

Le nouveau firmware ZLD 3.0 apporte de nouvelles fonctionnalités : un meilleur débit pour un réseau plus rapide et hautement sécurisé, une compatibilité IPv6 pour assurer les futurs investissements, des services UTM comme les licences anti-spam et filtrage de contenu de Commtouch, un support VPN SSL pour le partage de fichiers et bien plus encore ... Et le mieux dans tout cela ? Vous bénéficiez comme pour l'ensemble des produits ZyXEL, de mises à jour majeures de firmware gratuitement, en téléchargement libre sur notre site.



La dernière fois, nous vous exposions les défis auxquels était confrontée une usine de chocolat. La tendance actuelle avec la multiplicité des filiales, travailleurs à domicile, itinérants, engendre de nouvelles exigences pour protéger et accéder en toute sécurité au réseau de l'entreprise.

C'est pourquoi, nous prenons aujourd'hui l'exemple d'une chaîne de supermarchés avec toutes ses spécificités.

Enfin, nous espérons que ce guide vous aidera à accompagner vos clients dans leurs démarches et à trouver la solution adaptée à leurs besoins en leur apportant une véritable solution sur mesure. Ce guide vous présente une multitude de scénarios possibles avec des descriptions détaillées de produits et des schémas applicatifs.

Salutations



Thorsten Kurpjuhn

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



Justin Lin

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

Cas client : une chaîne de supermarchés



Une chaîne de supermarchés d'une taille moyenne compte 20 employés sur le site central et 7 employés sur chacun des 5 sites. Elle propose ses produits directement dans ses supermarchés ou via sa boutique en ligne. Le gérant souhaite embaucher plusieurs télétravailleurs, freelancers ou designers qui auront besoin d'accéder au réseau de l'entreprise, et ce, de façon ponctuelle. L'entreprise se voit donc confrontée à plusieurs défis qui vous seront exposés dans ce guide.

Défi :

Les coupures d'accès à Internet engendrent des coûts conséquents pour l'entreprise. Nous avons vraiment besoin d'un accès permanent à Internet !

Solution :

Les différents ports WAN permettent à votre entreprise de rester connectée. Utilisez des connexions Internet redondantes ou la 3G en tant que ligne de secours.

Voir page 10

Défi :

L'accès à Internet est déployé via différents fournisseurs d'accès. Nous souhaitons pouvoir utiliser la bande passante et gérer les priorités afin d'offrir à nos clients un service de boutique en ligne disponible 24h/24.

Solution :

Grâce à la fonction de répartition de charge, vous pouvez gérer le trafic et la bande passante selon vos exigences. De plus, vous bénéficiez d'une meilleure qualité de services (QoS).

Voir page 11

Défi :

La migration vers l'IPv6 devient incontournable. Nous souhaitons que notre entreprise puisse bénéficier d'une solution évolutive et donc migrer à terme.

Solution :

Opter pour une appliance de sécurité certifiée "IPv6 ready" vous permettra de garantir la pérennité de votre installation. Cette certification ZyWALL USG vous assure une migration en douceur vers l'IPv6.

Voir page 12

Défi :

Nous souhaitons mettre à la disposition de nos clients un site web sécurisé et sans faille.

Solution :

La fonction NAT (Network Address Translation) permet aux clients d'accéder facilement aux serveurs FTP tout en protégeant votre réseau d'éventuelles menaces.

Voir page 13

Défi :

Notre entreprise possède cinq filiales. Nous souhaitons qu'elle puisse accéder au réseau du site central en toute sécurité.

Solution :

Le VPN IPSec vous permet d'établir des connexions sécurisées via Internet entre 2 sites. Les employés des filiales pourront ainsi accéder au réseau du siège très simplement. Il suffit pour cela d'installer un ZyWALL USG sur chaque site.

Voir page 14

Défi :

Parfait, comment faire alors ?

Solution :

Avec le logiciel client IPSec, vous leur permettez d'établir une connexion client-à-site. Grâce à la fonction Easy VPN disponible sur les ZyWALL USG, il est encore plus facile d'établir une connexion sur un client car le logiciel y est installé de manière automatisée, sans effort de configuration.

Voir page 15

Défi :

Notre entreprise travaille avec des freelances ayant besoin d'accéder à notre réseau mais ce, de manière ponctuelle.

Solution :

Dans ce cas, le VPN SSL est la solution idéale. En utilisant simplement leur navigateur Web, ils peuvent facilement accéder au ZyWALL USG et établir un tunnel sécurisé (similaire aux banques en ligne). Ne nécessitant aucune installation de logiciel, cette solution est simple et économique pour les personnes souhaitant utiliser temporairement les ressources de l'entreprise.

Voir page 16

Défi :

L'utilisation des smartphones ou tablettes est aujourd'hui un moyen largement répandu pour sernet. Nous souhaitons offrir ce service à nos employés et clients.

Solution :

Le VPN L2TP est préconisé pour les utilisateurs distants avec appareils mobiles qui souhaitent se connecter de manière sécurisée au réseau. Les appliances de sécurité ZyXEL supportent cette technologie de VPN L2TP pour permettre aux employés de se connecter en accès distant au site central de façon conviviale.

Voir page 17

Défi :

Nous utilisons la téléphonie sur IP (VoIP). Comment pouvons-nous bénéficier d'une bonne qualité audio ? Est-il possible de gérer la priorité de bande passante pour les utilisateurs les plus exigeants ?

Solution :

La fonctionnalité de gestion de la bande passante vous permet de prioriser le trafic important. Ceci évite que du trafic moins prioritaire ne vienne prendre les ressources de la bande passante. De plus, vous pouvez allouer la bande passante que vous souhaitez à chaque utilisateur et mettre en priorité les utilisateurs importants.

Voir page 18

Défi :

De plus en plus de nos employés utilisent des applications de peer to peer et les réseaux sociaux. Nous souhaitons les limiter afin qu'ils se recentrent sur leur activité professionnelle et que la bande passante soit utilisée de manière efficace.

Solution :

Le contrôle applicatif (Application Patrol) des ZyWALL USG vous donne un contrôle granulaire, par utilisateur, des applications IM (Messageries Instantanées) et P2P. Vous pouvez ainsi autoriser des applications nécessaires à l'entreprise pour des utilisateurs et pendant des plages horaires précises (la fonction IM/P2P nécessite une licence IDP).

Voir page 19

Défi :

Internet est aujourd'hui le vecteur privilégié pour propager des menaces contre les réseaux et autres logiciels malveillants. Nous souhaitons protéger nos collaborateurs des attaques malwares en provenance du Web.

Solution :

Nous vous recommandons un service de filtrage de contenu reposant sur une base évolutive d'utilisateurs. Ce dernier vous permet de détecter les menaces en temps réel, de bloquer les sites Web suspects et d'analyser les contenus en temps réel. Le filtrage de contenu met à jour automatiquement les signatures nécessaires afin de protéger l'ensemble du réseau contre les malwares et les attaques d'hameçonnage actuelles.

Voir page 20

Défi :

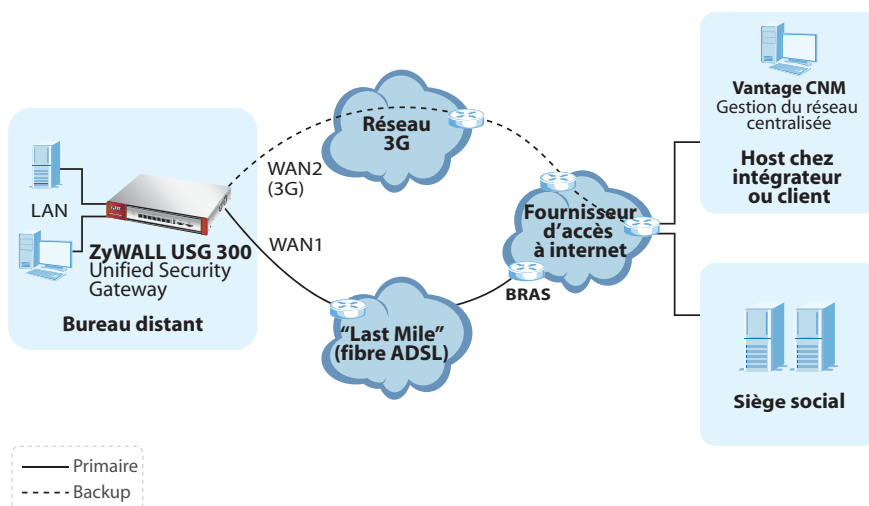
Nous sommes quotidiennement infesté de spam sur notre réseau. Ceci implique pour notre entreprise une perte significative de productivité.

Solution :

Nous vous recommandons notre service Anti-Spam qui signale ou bloque les mails à caractère publicitaire. C'est une solution idéale, performante avec des taux de détection efficaces.

Voir page 21

Connexion sans interruptions grâce aux fonctions backup



Solution

Un WAN (Wide Area Network) est un réseau informatique couvrant une grande zone géographique et qui interconnecte un réseau privé LAN (Local Area Network) et d'autres réseaux ou à Internet. Grâce au LAN, les PC sur un site peuvent communiquer avec les PC d'autres sites. Les ZyWALL USG incluent une fonction WAN multiples qui leur permet de raccorder jusqu'à deux opérateurs ou réseaux IP par le biais de connexions Ethernet, PPPoE ou 3G. Les utilisateurs peuvent utiliser les trunks soit pour la répartition de charge

du trafic WAN afin d'augmenter le débit global du réseau, soit en tant que ligne de secours afin d'améliorer la fiabilité de la connexion Internet. La répartition de charge sera expliquée en détail à la page suivante (Scénario 2). Le graphique ci-dessus montre comment un USG assure la continuité de service avec une connexion PPPoE comme WAN primaire et des connexions 3G via USB en tant que lignes de secours. En général, l'USG se connecte à Internet via la connexion PPPoE privilégiée avec capacité de basculer vers un WAN 3G secondaire en cas de perte de connexion.

Principales caractéristiques

- Ports WAN multiples pour répartition de charge et en cas de coupure
- Connexion Internet sans interruption grâce aux WAN multiples et lignes de secours 3G
- Support des deux modes suivants :
 - actif actif pour répartition de charge
 - actif passif en cas de coupure
- Les ZyWALL USG sont compatibles avec divers cartes 3G (vous trouverez la liste actualisée sur www.zyxel.com)

Avantages

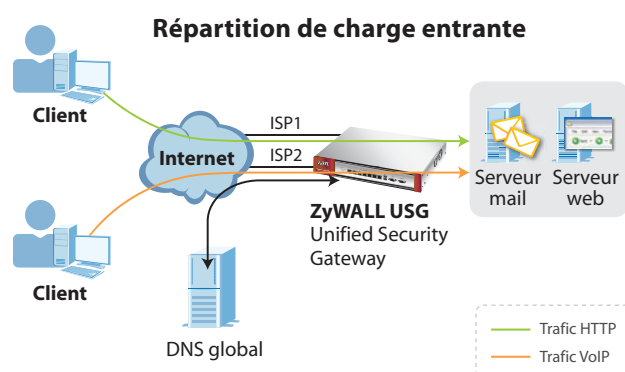
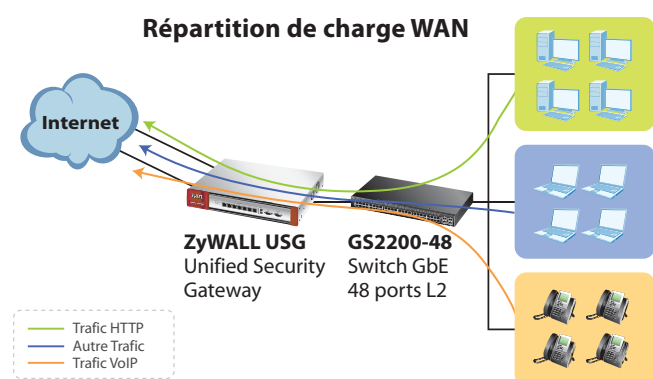
- Un travail sans interruption d'activité en cas de perte de ligne de la connexion principale
- La ligne 3G flexible peut être utilisée en tant que connexion Internet de secours, ce qui assure une continuité de service optimale
- Des connexions fiables au sein du réseau d'entreprise

Connexions Internet performantes

Solution

En tant que passerelles professionnelles, les ZyWALL USG supportent en général plusieurs connexions WAN. Sans répartition de charge, une connexion WAN risque de devenir un goulot d'étranglement et de ralentir considérablement le trafic sur le réseau. C'est pourquoi les données sortantes sont réparties sur plusieurs connexions Internet par l'USG. Ce procédé nommé équilibrage de charge garantit que les données puissent passer le pare-feu sans interruption et que la connexion Internet soit utilisée plus efficacement pour améliorer les performances des applications. Les ZyWALL USG sont capables de différencier les types de trafic tels que

la voix sur IP ou le trafic http et de les transmettre à un WAN précis en cas de besoin. Pour fournir aux clients un service sans interruption, les USG offrent également l'équilibrage de charge entrante. Chaque requête DNS est traitée sur le port utilisant le moins de ressource, c'est à dire qui traite le moins d'adresses IP. Les paquets de données sont envoyés directement sur le port libre et non sur un port déjà surchargé. L'USG peut donc répondre à une requête DNS via une autre IP WAN. Cela permet aux clients d'avoir immédiatement accès aux serveurs qui se situent derrière l'USG.



Principales caractéristiques

- Solution flexible pour répartition de charge
- Algorithmes de Load Balancing :
 - Weighted Round Robin (WRR), répartition à l'aide d'une relation définie
 - Least Load First (LLF), connexion la moins chargée
 - Spillover (par débordement)

Avantages

- Augmentation du débit et de la résilience
- Des clients satisfaits grâce à l'accès rapide aux serveurs
- Contrôle et sécurité des applications
- Répartition de charge entrante DNS

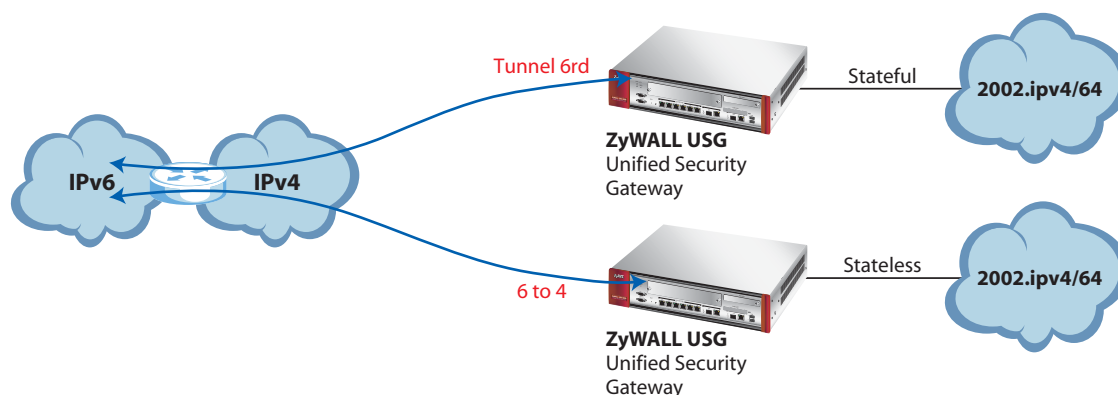


Compatibilité et migration IPv6 en toute simplicité

Solution

Les ZyWALL USG sont conformes aux normes du forum IPv6 et ont obtenu la certification IPv6 Ready (phases 1 et 2). Le forum IPv6 est un consortium international qui a pour but de favoriser la migration vers le nouveau protocole.

Lorsque la fonction IPv6 est activée sur le pare-feu, l'USG attribue des adresses IPv6 aux clients connectés, ce qui permet de transmettre du trafic IPv6 à travers une infrastructure IPv4. Les USG supportent le Dual Stack et le tunneling IPv4 (6rd et transition 6to4) pour assurer une connexion Internet vers des équipements IPv6.



Principales caractéristiques

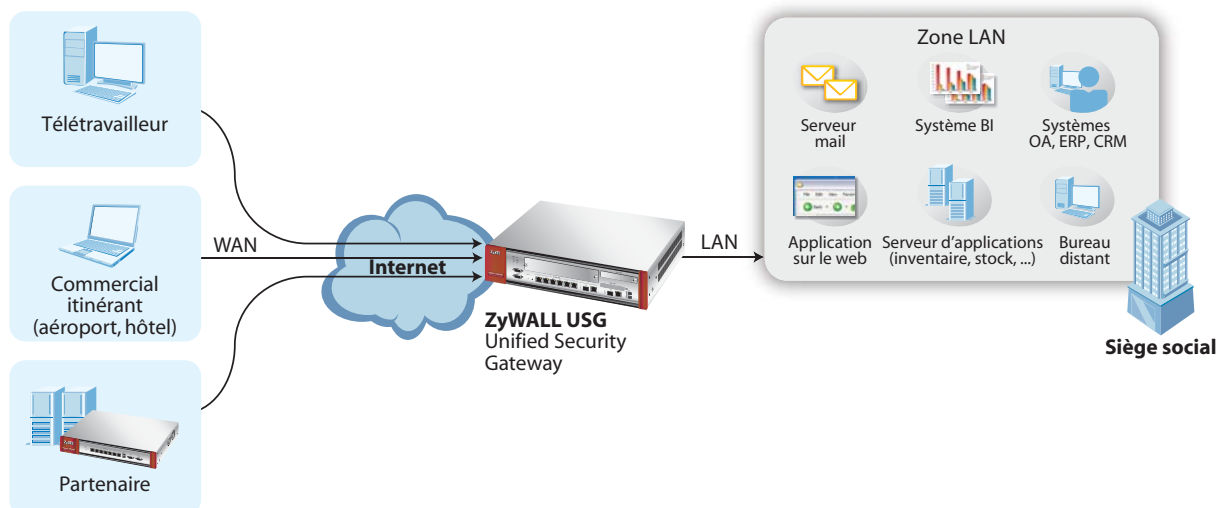
- Certification IPv6 Ready
- Support Dual Stack, 6rd (déploiement IPv6 rapide) et tunnel de transition 6 à 4 pour le WAN
- Support IPv6 stateful/stateless et DHCPv6 pour le LAN
- Support pare-feu IPv6



Avantages

- Les ZyWALL USG sont conformes aux normes industrielles actuelles
- Migration conviviale vers l'IPv6
- Architecture évolutive et investissements durables

Sécurité maximale depuis un serveur



Solution

Le NAT (Network Address Translation) est le processus qui remplace l'adresse IP d'un hôte par une autre dans un paquet IP. La fonction NAT permet aux ordinateurs d'un réseau privé derrière un USG d'être accessibles de l'extérieur.

Afin de répondre aux besoins les plus critiques en matière de sécurité tout en permettant aux clients ou serveurs sur le réseau public (WAN) d'accéder au réseau privé (Intranet), il est recommandé de placer les serveurs derrière un USG. Une entreprise peut disposer d'un serveur FTP qui doit être accessible par les utilisateurs nomades. Pour répondre à cette demande, l'administrateur doit simplement paramétrer une règle NAT pour transmettre le trafic de l'Internet vers l'Intranet.

Principales caractéristiques

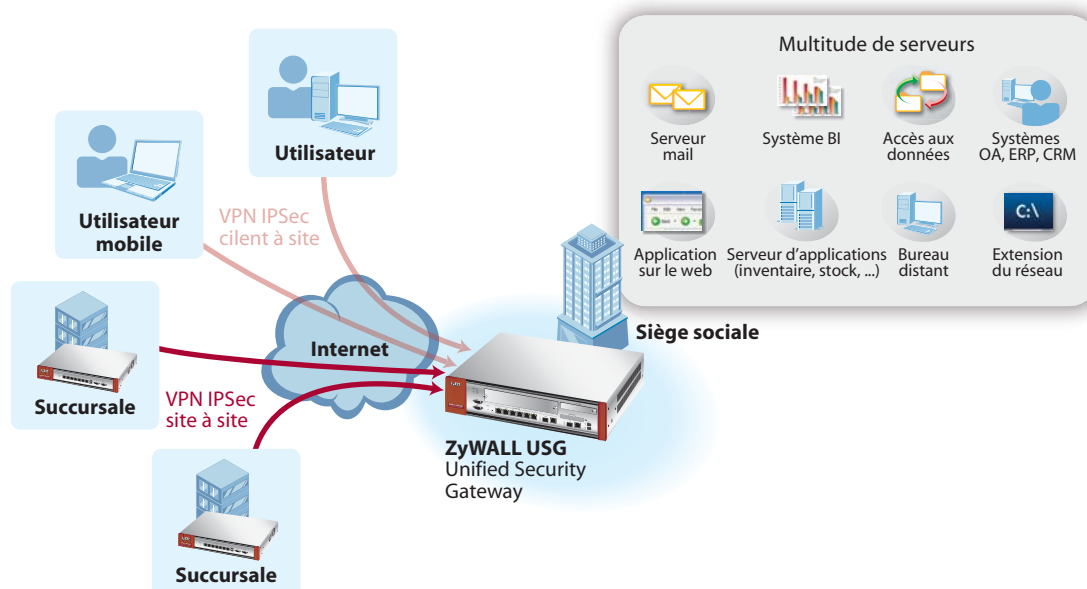
- Support NAT/PAT et NAT sur des règles (SNAT)
- Support Loopbacks One-to-One, Many-to-One et NAT

Avantages

- Haute disponibilité du réseau
- Empêche les attaques en provenance de l'extérieur en masquant la véritable adresse IP du serveur.



Interconnexion sécurisée entre deux sites



Solution

L'Internet Protocol Security (IPSec) est un standard VPN qui assure des connexions privées et protégées sur des réseaux publics comme Internet. Un tunnel VPN IPSec est habituellement établi en deux phases; dans chaque phase, une security association (SA) est mise en place. Une SA est l'établissement des paramètres de sécurité partagés entre le ZyWALL et le routeur IPSec sur le site déporté. Lors de la première phase, l'Internet Key Exchange (IKE) SA est établi entre l'USG et le routeur situé sur l'autre extrémité du réseau. En deuxième phase, la SA IKE permet d'établir une SA IPSec sécurisée pour échanger des données entre les ordinateurs sur le réseau local et ceux du réseau déporté. Une connexion VPN IPSec permet donc aux entreprises d'assurer une connexion sécurisée optimale entre le site central et leurs succursales ou partenaires.



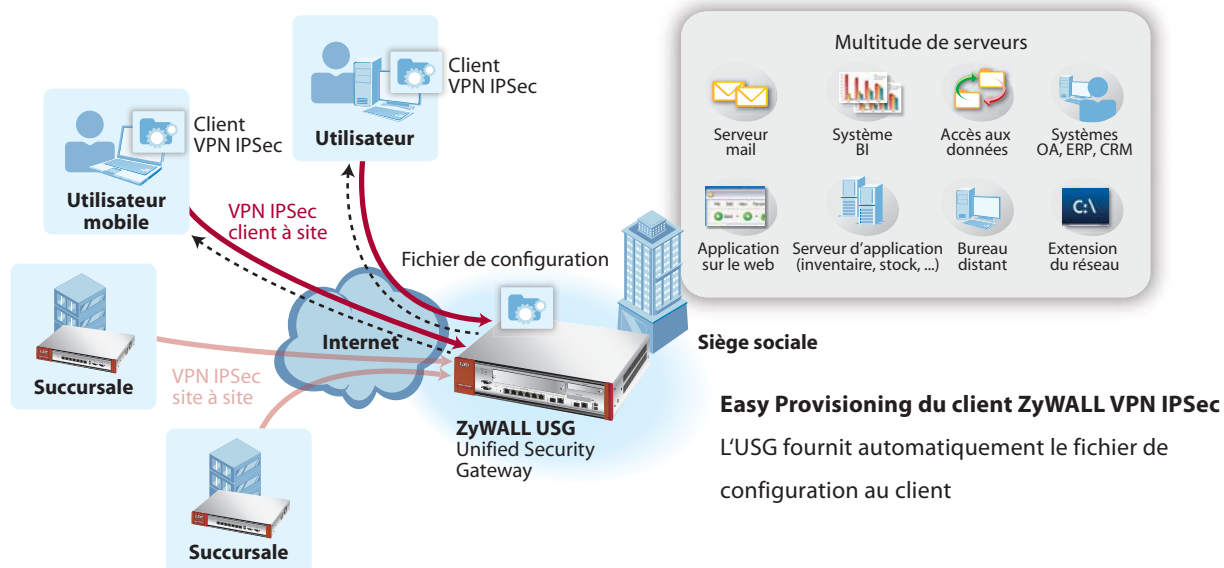
Principales caractéristiques

- VPN IPSec certifié ICSA
- Supporte les algorithmes suivants : AES/3DES/DES
Authentification : SHA-1/MD5

Avantages

- Solution simple et à moindre coût pour une connexion sécurisée entre le site central et les sites déportés
- Connexions sécurisées cryptées sur Internet
- Connectivité toujours disponible

Connexion sécurisée pour les utilisateurs nomades



Solution

Les collaborateurs itinérants ou ceux qui travaillent à domicile peuvent accéder très simplement au réseau de l'entreprise via une connexion VPN SSL ou IPSec. Les ZyWALL USG supportent la technologie VPN SSL qui permet aux collaborateurs, revendeurs ou partenaires d'accéder en toute convivialité aux ressources de l'entreprise sans avoir à installer de logiciel sur les postes clients. Solution idéale pour une connexion sécurisée et conviviale, le VPN SSL peut être déployé sur des entreprises de toutes tailles.

Bien que l'établissement d'un tunnel VPN soit une solution conviviale pour une PME, elle peut également s'avérer difficile à mettre en place pour du personnel non technique comme des commerciaux. Equipé de la fonction Easy VPN, l'USG peut fournir automatiquement les données de configuration au client distant. Cette facilité de déploiement réduit sensiblement les coûts liés à la configuration tout en sécurisant l'accès.

Principales caractéristiques

- Fonction d'auto provisioning pour le VPN IPSec
- Préconfiguration pour un déploiement en masse
- Easy VPN compatible avec tous les ZyWALL USG

Avantages

- Accès à distance sans effort de configuration
- Frais d'installation réduits
- Solution conviviale : installer, redémarrer et ça fonctionne !



Accès à distance sur le Web avec règles individuelles

Solution

Un accès VPN SSL est la solution idéale pour mettre en place un accès distant sur le Web. Les freelances ou utilisateurs itinérants peuvent ainsi établir un tunnel sécurisé entre leur ordinateur et le ZyWALL USG via le navigateur Web (même procédé que pour les banques en ligne). Ne nécessitant aucun logiciel, le VPN SSL représente un moyen simple et à moindre coût pour accéder au réseau de l'entreprise pour des personnes qui n'ont que rarement besoin des ressources de l'entreprise.

Grâce à la fonction VPN SSL, les ZyWALL USG permettent aux utilisateurs d'accéder au réseau en toute convivialité via un tunnel sécurisé. Tout ce qui est requis est un navigateur web sur le PC de l'utilisateur. En outre, le VPN SSL permet à l'administrateur du réseau de définir des règles d'accès personnalisées et d'établir des profils d'utilisateurs différents, ce qui garantit l'accès à différentes ressources de l'entreprise en fonction du profil. Par exemple, un administrateur réseau peut établir une règle de VPN SSL autorisant un responsable à gérer à distance les serveurs de l'entreprise via RDP ou VNC. De même, il peut définir une règle VPN SSL autorisant l'équipe commerciale à accéder aux données dont ils ont besoin quotidiennement.

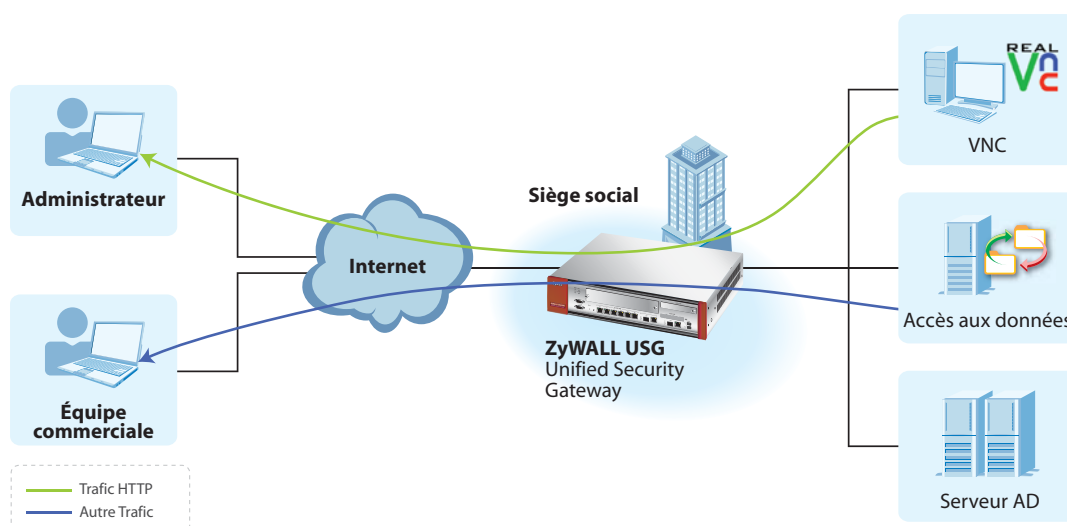


Principales caractéristiques

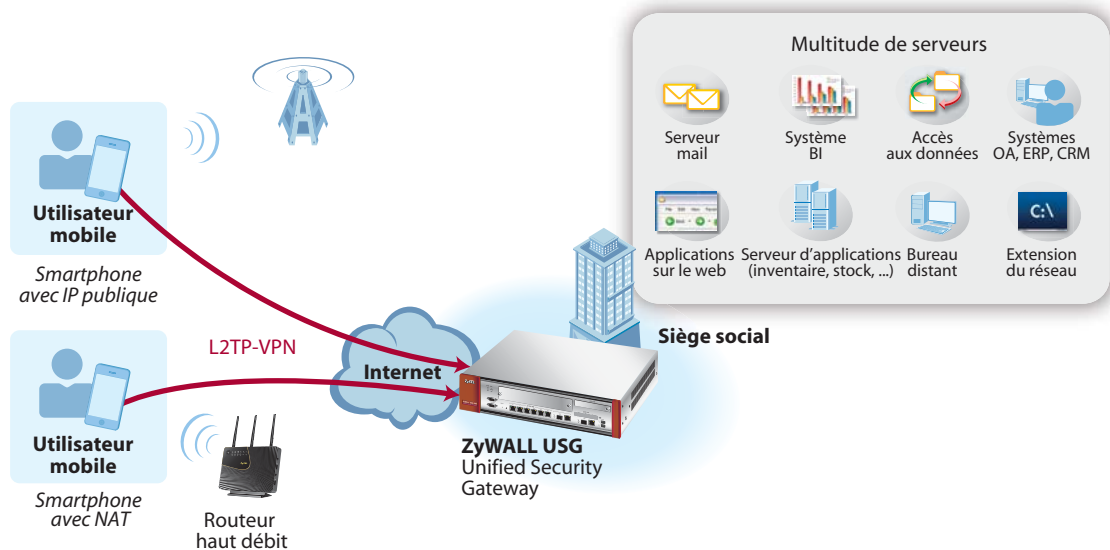
- Accès à distance sans installation de logiciel client
- Modes VPN SSL supportés : Reverse Proxy et Full Tunnel
- Page d'accueil personnalisable
- Utilisation conviviale via navigateur Web

Avantages

- Coûts d'installation et d'assistance technique réduits comparés aux clients VPN traditionnels.
- Installation simple et rapide, diagnostic simplifié



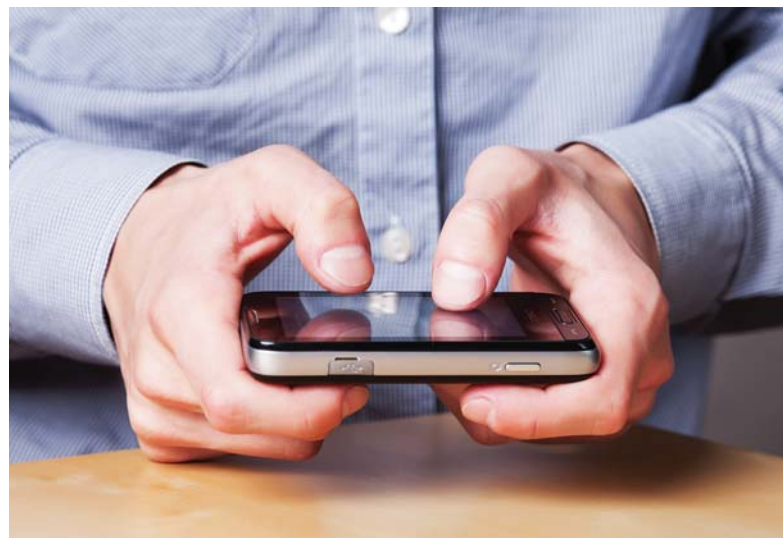
Accès à distance avec appareils mobiles et smartphones



Solution

Une connexion VPN L2TP est utilisée par les utilisateurs distants qui possèdent des services mobiles pour se connecter au réseau depuis le ZyWALL USG. L'utilisateur distant n'a pour cela ni besoin de passerelle IPSec, ni de logiciel client VPN.

La série ZyWALL USG supporte la technologie VPN L2TP sur les iPhone, android et beaucoup d'autres terminaux mobiles, permettant ainsi aux utilisateurs distants d'accéder très simplement au site central. Les USG supportent le transfert de données sécurisées même si le terminal utilise la fonction NAT.



Principales caractéristiques

- L2TP sur IPSec pour terminaux iOS et android
- Support iOS 4 et iOS 5
- Support Android 2.2 et 2.3

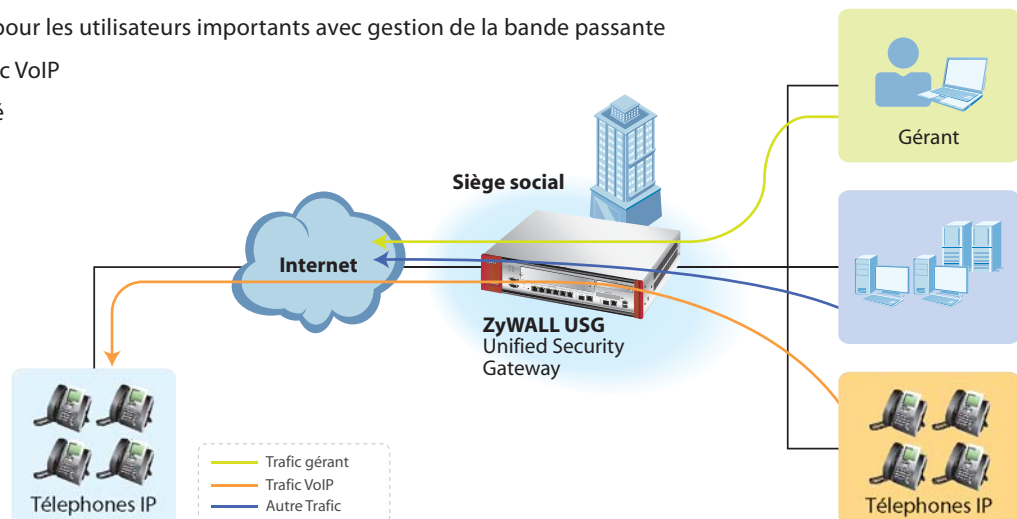
Avantages

- Accès à distance plus convivial
- Rentabilité optimisée
- Accès sécurisé aux ressources de l'entreprise, n'importe quand et n'importe où

Gestion de la bande passante et des applications sensibles

Priorisation du trafic par utilisateur ou selon le type de trafic

- Mise en priorité du trafic pour les utilisateurs importants avec gestion de la bande passante
- Priorité haute pour le trafic VoIP
- Nombre de sessions limité



Solution

Il existe différents types de trafic sur le réseau d'une entreprise. La bande passante étant souvent limitée, certains trafics ou des utilisateurs en charge de tâches importantes doivent bénéficier d'une haute priorité et d'une transmission des données fiable.

Les ZyWALL USG disposent d'une fonction de gestion de la bande passante (Bandwidth Management, BWM) permettant de gérer de manière optimale la bande passante en fonction de critères flexibles. Par exemple, le trafic VoIP étant plus sensible à des latences, il prend généralement la plus haute priorité du réseau d'une entreprise. De plus, la fonction de gestion de la bande passante permet d'attribuer une bande passante prioritaire aux utilisateurs importants. L'administrateur réseau peut par exemple limiter le nombre de sessions par utilisateur pendant les heures de travail, dans le but d'empêcher une sur-consommation de la bande passante par un seul utilisateur.



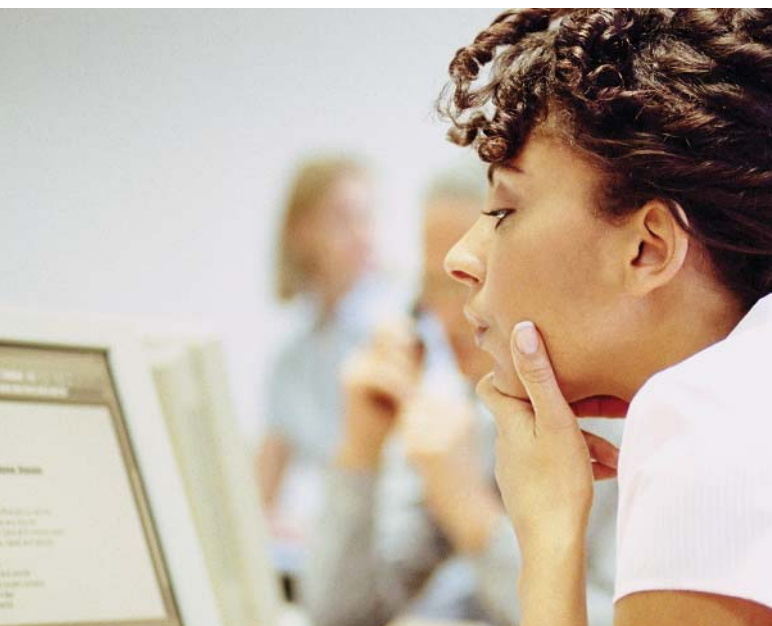
Principales caractéristiques

- Gestion de la bande passante (BWM)
- Bande passante allouée au trafic VoIP
- Continuité de service pour les utilisateurs importants grâce à la gestion prioritaire de leurs applications

Avantages

- Excellente Qualité de Service VoIP (QoS)
- Connexion Internet priorisée pour les utilisateurs importants
- Gestion plus efficace de la bande passante disponible
- Réduction des coûts grâce à la gestion de la bande passante

Optimisation de la rentabilité et productivité des utilisateurs



Solution

Les entreprises perdent en productivité lorsque les utilisateurs utilisent leur temps de travail pour le chat, le téléchargement de fichiers illégaux ou la consultation de sites de réseaux sociaux comme Facebook ou Twitter. Cette utilisation intempestive de la bande passante engendre non seulement une perte de productivité pour l'entreprise mais pèse également sur les ressources Internet.

La fonction Application Patrol permet de contrôler la messagerie instantanée (IM), le P2P (Peer to Peer) et les réseaux sociaux par utilisateur. Il est également possible de limiter la bande passante pour ce type d'applications (les services de IM/P2P nécessitent l'achat d'une licence IDP).



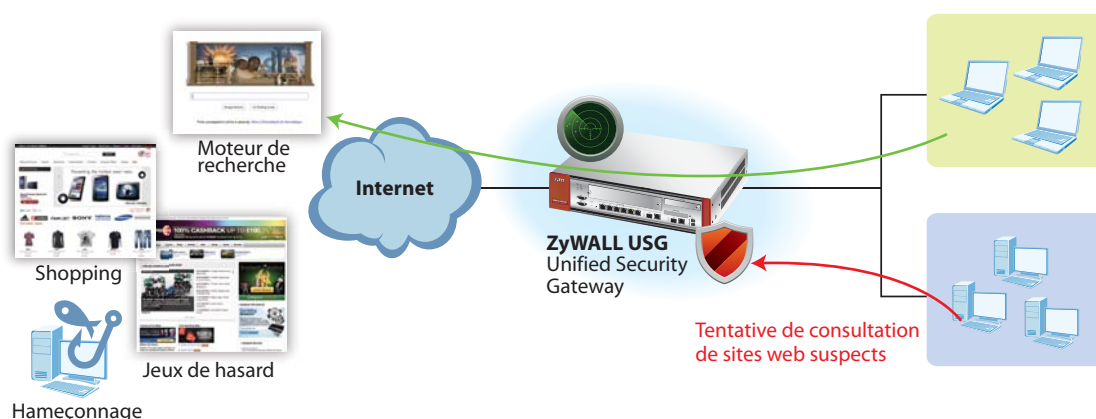
Principales caractéristiques

- Contrôle granulaire d'applications diverses (IM/P2P, flux média, voix sur IP etc.)
- Support de nombreuses applications IM et P2P
- Bande passante maximale / réservée
- Les ZyWALL USG 2000/1000/300/200/100/50 supportent la fonction Application-Patrol

Avantages

- Economies réalisées par l'entreprise et meilleure productivité
- Règles par utilisateur ou groupe d'utilisateurs (profils individuels)
- Limitation des menaces en empêchant une utilisation abusive d'Internet
- Contrôle de l'ensemble du réseau

Filtrage de contenu et protection contre les malwares



Solution

Le filtrage de contenu implémenté dans la série ZyWALL USG est la solution idéale pour lutter contre la diversité, rapidité et constantes évolutions des menaces en ligne reposant sur une grande communauté d'utilisateurs.

■ Identification des nouvelles menaces en temps réel :

les experts de la sécurité en ligne et moteurs de détection de menaces proposent une analyse détaillée, en temps réel et fiable des contenus Web, URLs, adresses IP et protocoles .

- Sécurité améliorée : les solutions de sécurité basées sur le cloud sont conçues pour se prémunir des incidents, analyser, classer et bloquer les malwares avant même qu'ils ne se répandent sur les réseaux et infectent les systèmes.

Développé par les principaux fournisseurs de solutions de sécurité CommTouch et Blue Coat, le service de filtrage de contenu de ZyXEL permet d'optimiser les coûts et garantit une protection du réseau en s'appuyant sur une base de données de millions d'URL, d'adresses IP continuellement mises à jour.

Principales caractéristiques

- Filtrage de contenu Blue Coat/CommTouch optionnel
- Permet sur le Web 2.0 le filtrage des pages à contenu multi-source (par. ex. les forums) en bloquant les contenus dynamiques
- Compatible avec le logiciel de reporting Vantage Report qui assure une surveillance et analyse complètes des activités Web et détecte les risques potentiels.
- Gestion centralisée via ZyXEL Vantage CNM

Avantages

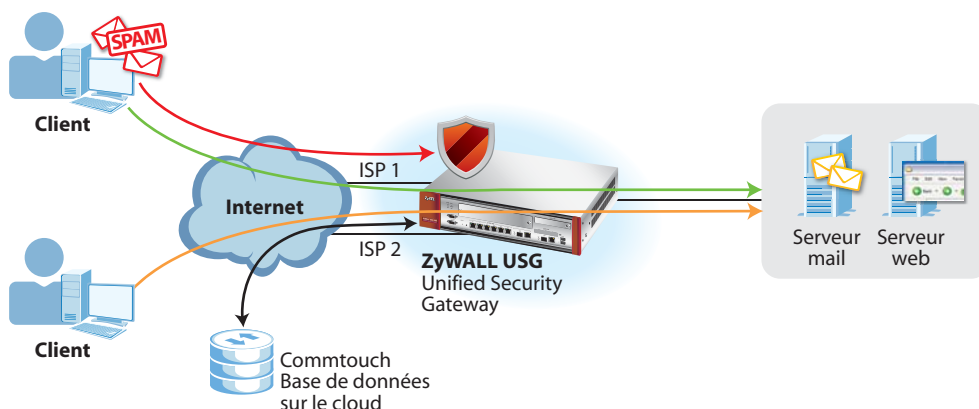
- Protection contre les malwares : protection du réseau en temps réel contre les malwares et attaques d'hameçonnage
- Améliorer la productivité : contrôle et blocage de sites suspects pour augmenter la productivité des employés.
- Gestion de la bande passante : identifie les sites hautement consommateurs de bande passante (par ex les films, téléchargement de musiques etc.)

Anti-spam pour meilleure protection des données confidentielles



Solution

Une protection contre les spam est aujourd'hui une stratégie incontournable à adopter pour la protection de votre réseau face à l'envoi massif et journalier de courriers indésirables, inappropriés ou même nocifs. Les spams mobilisent en effet les ressources et sont une perte de temps à gérer, et donc de productivité pour les employés. Les ZyWALL USG disposent d'un service anti-spam qui permet ainsi de stopper les menaces et protéger au mieux le réseau de l'entreprise.



Principales caractéristiques

- Technologie anti-spam CommTouch
- Technologie RDP innovante CommTouch : détecte et bloque les envois en masse en temps réel
- Filtrage selon la source IP de l'émetteur : bloque plus de 80 % des e-mails indésirables
- Zero Hour Virus Outbreak Protection: les ZyWALL USG bloquent les e-mails suspects avant même que des signatures officielles ne soient disponibles

Avantages

- Optimisation de vos ressources et de la sécurité de vos données
- Bande passante élevée, performances améliorées
- Sécurité des données optimisée



Aperçu des produits



■ Unified Security Gateways pour TPE

La série ZyWALL USG 20/20W/50/100/200 est conçue pour les TPE et PME qui souhaitent contrôler en temps réel leur réseau et qui ont besoin d'une protection à plusieurs niveaux contre les menaces les plus diverses en provenance du Web. La série intègre un pare-feu SPI (Stateful Packet Inspection), supporte l'anti-virus, l'IDP (Détection et prévention d'intrusion), le filtrage de contenu, l'anti-spam et le VPN (IPSec/SSL/L2TP).

Caractéristiques

- Protection renforcée et excellente performance réseau
- Support IPv6
- Accès à distance simplifiée et sans configuration grâce à Easy VPN
- VPN L2TP pour appareils mobiles (iPhone et Android)
- Pare-feu ICSA, certification IPSec
- Filtrage de contenu contre les malwares et menaces en provenance du Web
- Continuité du service Internet grâce à la répartition de charge et la ligne de secours 3G



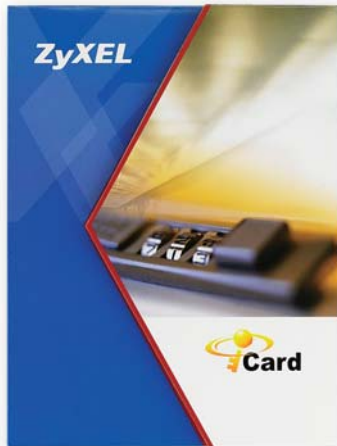
■ Unified Security Gateways pour PME

Les plates-formes de sécurité ZyWALL USG 300/1000/2000 se distinguent par de très hautes performances. Ils détectent les paquets de données grâce à la fonction Deep Packet Inspection en offrant une protection efficace contre les accès non autorisés et les menaces en provenance du web comme les virus, vers, attaques d'hameçonnage, spams et toutes sortes de malwares. De plus, ils garantissent des connexions à distance sécurisée site-à-site entre entreprises, partenaires et clients.

Caractéristiques

- Protection renforcée et performance
- Support IPv6
- Accès à distance simplifiée et sans configuration grâce à Easy VPN
- VPN L2TP pour appareils mobiles (iPhone et Android)
- Pare-feu ICSA, certification IPSec
- Protection dynamique contre les malwares en temps réel
- High Availability HA (haute disponibilité)





■ Licences de sécurité et services

Les ZyWALL USG supportent de nombreux services de sécurité qui peuvent être activés en achetant les licences correspondantes. Les services UTM sont constamment actualisés grâce à un serveur fonctionnant 24h/24 fournissant aux utilisateurs du monde entier des mises à jour de base de signatures.

Licences de sécurité disponibles

- Service anti-virus Kaspersky & ZyXEL
- Détection et prévention d'intrusion (IDP)
- Service filtrage de contenu Blue Coat ou CommTouch
- Service anti-spam CommTouch
- VPN SSL
- Client VPN IPSec



■ Vantage Report

Cet outil de reporting génère des rapports automatiques et présente sous forme de graphiques les activités de sécurité anti-virus, anti-spam, filtrage de contenu et IDP des ZyWALL USG. Vantage Report permet de tracer le trafic qui transite à travers les USG se trouvant sur différents sites.

Caractéristiques

- Grande variété de rapports graphiques
- Interface utilisateur Web (application sur navigateur)
- Manipulation simple et intuitive
- Envoi de rapports de manière périodique et automatisée



■ Vantage CNM

Vantage CNM est un logiciel d'administration sur le Web pour fournisseurs de services et responsables IT. Les pare-feux ZyWALL peuvent ainsi être configurés et surveillés de manière centralisée.

Caractéristiques

- Gestion centralisée
- VPN One Click et gestion VPN graphique
- Déploiement / gestion de règles ACL applicables sur plusieurs pare-feu simultanément



Corporate Headquarters

ZyXEL Communications Corp.

Tel: +886 3 578 3942
Fax: +886 3 578 2439
Email: sales@zyxel.com.tw
www.zyxel.com

■ Asia

ZyXEL China (Shanghai)

China Headquarters
Tel: +86 21 6119 9055
Fax: +86 21 5206 9033
Email: sales@zyxel.cn
www.zyxel.cn

ZyXEL China (Beijing)

Tel: +86 10 6260 2249
Email: sales@zyxel.cn
www.zyxel.cn

ZyXEL China (Tianjin)

Tel: +86 22 8789 0440
Fax: +86 22 8789 2304
Email: info@zyxel.cn
www.zyxel.cn

ZyXEL India

Tel: +91 11 4760 8800
Fax: +91 11 4052 3393
Email: info@zyxel.in
www.zyxel.in

ZyXEL Kazakhstan

Tel: +7 727 259 0699
Email: info@zyxel.kz
www.zyxel.kz

ZyXEL Malaysia

Tel: +60 3 7960 0088
Fax: +60 3 7960 8802
Email: info@zyxel.com.my
www.zyxel.com.my

ZyXEL Pakistan

Tel: +92 21 3431 0194-5
Fax: +92 21 3431 0196
Email: info@zyxel.com.pk
www.zyxel.com.pk

ZyXEL Singapore

Tel: +65 6899 6678
Fax: +65 6899 8887
Email: sales@zyxel.com.sg
www.zyxel.com.sg

ZyXEL Taiwan (Taipei)

Tel: +886 2 2739 9889
Fax: +886 2 2735 3220
Email: sales_tw@zyxel.com.tw
www.zyxel.com.tw

ZyXEL Thailand

Tel: +66 2 831 5315
Fax: +66 2 831 5395
Email: info@zyxel.co.th
www.zyxel.co.th

■ Europe

ZyXEL Belarus

Tel: +375 17 334 6099
Email: sales@zyxel.by
www.zyxel.by

ZyXEL BeNeLux

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

ZyXEL Bulgaria

Tel: +359 2 444 3343
Email: info@zyxel.bg
www.zyxel.bg

ZyXEL Czech Republic

Tel: +420 2 4109 1350
Fax: +420 2 4109 1359
Email: info@cz.zyxel.com
www.zyxel.cz

ZyXEL Denmark A/S

Tel: +45 3955 0700
Email: sales@zyxel.dk
www.zyxel.dk

ZyXEL Estonia

Tel: +372 622 6380
Email: tech@zyxel.ee

ZyXEL Finland

Tel: +358 9 4780 8400
Email: myynti@zyxel.fi
www.zyxel.fi

ZyXEL France

Tel: +33 47 252 9797
Fax: +33 47 252 1920
Email: info@zyxel.fr
www.zyxel.fr

ZyXEL Germany GmbH

Tel: +49 2 4056 9090
Fax: +49 2 4056 9099-9
Email: sales@zyxel.de
www.zyxel.de

ZyXEL Hungary & SEE

Tel: +36 1 336 1640
Fax: +36 1 325 9100
Email: info@zyxel.hu
www.zyxel.hu

ZyXEL Italy

Tel: 800 992 604
Fax: +39 011 274 7647
Email: sales@zyxel.it
www.zyxel.it

ZyXEL Latvia

Tel: +371 6 601 3019
Email: tech@lv.zyxel.com

ZyXEL Lithuania

Tel: +370 5205 4297
Email: tech@lt.zyxel.com

ZyXEL Norway

Tel: +47 2 280-6180
Fax: +47 2 280-6181
Email: salg@zyxel.no
www.zyxel.no

ZyXEL Poland

Tel: +48 22 333 8250
Fax: +48 22 333 8251
Email: info@pl.zyxel.com
www.zyxel.pl

ZyXEL Romania

Tel: +40 31080 9888
Fax: +40 31080 9890
Email: info@ro.zyxel.com
www.zyxel.ro

ZyXEL Russia

Tel: +7 495 542 8920
Fax: +7 495 542 8925
Email: info@zyxel.ru
www.zyxel.ru

ZyXEL Slovakia

Tel: +421 2 4319 3989
Fax: +421 2 4319 3990
Email: info@sk.zyxel.com
www.zyxel.sk

ZyXEL Spain

Tel: +34 91 300 5345
Fax: +34 91 300 5345
Email: sales@zyxel.es
www.zyxel.es

ZyXEL Sweden

Tel: +46 8 5577 6060
Fax: +46 8 5577 6061
Email: sales@zyxel.se
www.zyxel.se

ZyXEL Switzerland

Tel: +41 44 806 5100
Fax: +41 44 806 5200
Email: info@zyxel.ch
www.zyxel.ch

ZyXEL Turkey A.Ş.

Tel: +90 212 314 1800
Fax: +90 212 220 2526
Email: bilg@zyxel.com.tr
www.zyxel.com.tr

ZyXEL UK Ltd.

Tel: +44 1189 121 700
Fax: +44 1189 797 277
Email: sales@zyxel.co.uk
www.zyxel.co.uk

ZyXEL Ukraine

Tel: +380 44 494 4931
Fax: +380 44 494 4932
Email: sales@ua.zyxel.com
www.ua.zyxel.com

■ The Americas

ZyXEL USA

North America Headquarters
Tel: +1 714 632 0882
Fax: +1 714 632 0858
Email: sales@zyxel.com
www.us.zyxel.com

Plus d'informations sur : www.zyxel.fr

Copyright © 2012 ZyXEL Communications Corp. Tous droits réservés. ZyXEL et le logo ZyXEL sont des marques déposées de ZyXEL Communications Corp. Toutes les autres marques, tous les autres noms de produits sont propriétés de leurs propriétaires respectifs. Toutes les données techniques peuvent être modifiées sans préavis.