STUDERUS
network technologies

POINT.

Le magazine d'expertise dans la sécurité IT et les technologies de réseau

Faire le point sur les points forts

Série switch d'accès XGS2220

Comment protéger le pare-feu des attaques

Bien configurer le pare-feu

Comment devenir un fournisseur de services gérés

Édition avril 2023

SWITCH

ZYXEL

Série switch d'accès XGS2220

Avec les six modèles de la famille switch XGS2220, Zyxel fournit des switch d'accès couche 3 qui supportent Nebula et ont suffisamment de puissance PoE pour des points d'accès avec du WiFi 6 et 6E.

La série XGS2220
La série XGS2220 est le successeur officiel de la série XGS2210 et se caractérise par quelques améliorations considérables. La série comprend six modèles avec des versions PoE, des versions non-PoE et une version fibre. Ce qui est nouveau et possible sans problèmes avec les modèles de XGS2220 est la possibilité de gérer les switch via le portail de cloud Nebula.

Des versions non-PoE
Les modèles XGS2220-30 et XGS2220-54 offrent des ports 24 ou 48 Gigabit et sont conçus pour l'utilisation comme switch d'accès. Sa forme compacte permet l'utilisation de jusqu'à 54 ports sur une seule unité de hauteur dans le rack 19". Une option d'application typique est celle des réseaux clients exigeants qui demandent des fonctions couche 3 tels que des VLAN basés sur Subnet/Protocol/Mac ou des DHCP Server Guard et qui ne contiennent pas des appareils PoE.

Des versions PoE
Toutes les fonctionnalités des versions non-PoE font partie intégrante des modèles PoE XGS2220-30-HP, XGS2220-54HP et XGS2220-54FP. Ils offrent en plus Power over Ethernet. Ils sont déjà adaptés pour l'approvisionnement des appareils avec du WiFi 6, 6E et 7. Ils offrent du PoE++ sur 10 ports (IEEE 802.3bt) avec jusqu'à 60W par port et du PoE+ sur d'autres 16/40/40 ports (IEEE 802.3at) avec jusqu'à 30W par port. De plus, ils disposent des vastes budgets PoE de 400W, 600W et lors de la version puissance maximale même de 960W. En raison de la possibilité d'alimenter les appareils en mode consommation, ces budgets sont suffisants pour couvrir l'ensemble des scénarios possibles. Un scénario d'application typique est celui des environnements avec une multitude d'appareils PoE qui consomment beaucoup tels que des points d'accès WiFi 6/6E ou des caméras IP à haute définition lors des conférences vidéo, dans lesquelles les fonctionnalités couche 2 multidiffusion peuvent être utilisées.

Des versions fibre
Le modèle fibre XGS2220-30F offre 24 ports SFP 24 Gigabit avec une flexibilité maximale de l'interface qui permet un accès fibre direct ou des ports Base-T RJ-45 par des émetteurs-récepteurs correspondants. En outre, les deux ports uplink Ethernet multi-Gigabit 10G permettent un accès rapide et facile à des réseaux RJ-45 existants ou l'intégration performante des utilisateurs réseau à forte utilisation en bande passante au niveau switch d'accès. Une option d'application typique est l'emplacement entre le switch d'accès et le switch cœur de réseau dans la couche d'agrégation ou directement entre le pare-feu et la couche d'accès (souvent dans des environnements plus petits). Grâce aux 24 ports SFP, une multitude de switch d'accès peuvent être insérés directement. En cas de besoin de bandes passantes élevées, il est également possible de les raccorder directement via les ports uplink 10GB.

Les fonctionnalités de tous les six modèles :
Un système de ventilation intelligent
Pour la série XGS2220 aussi, Zyxel mise sur la technologie de ventilation intelligente éprouvée. Grâce à des capteurs de température et à un contrôle intelligent des ventilateurs qui adapte automatiquement la vitesse, les switch fonctionnent le plus silencieusement possible.

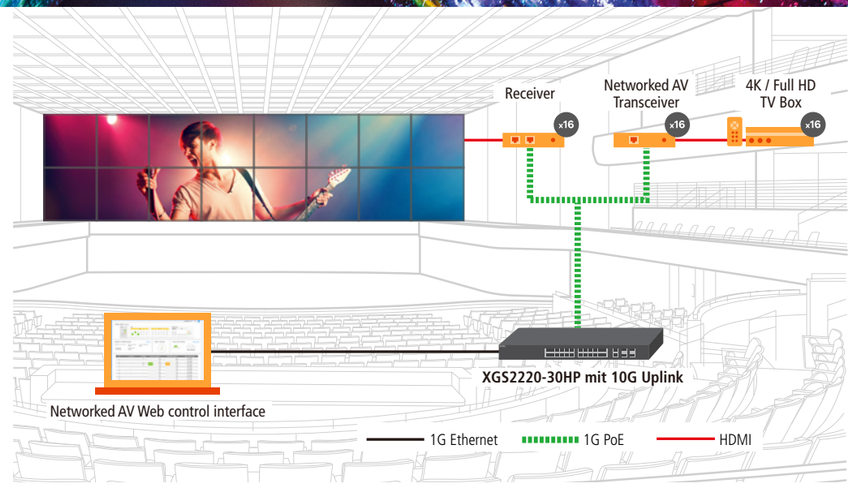
Des ports uplink
Par rapport à la série précédente, la nouvelle série XGS2220 dispose de six au lieu de quatre ports uplink 10 Gigabit ce qui augmente le débit uplink de 50 %. La flexibilité de connexion a aussi été augmenté en intégrant des ports RJ-45 2x 10G (1G/2.5G/5G/10G) en plus des ports 4x SFP+. Une autre option d'application est l'intégration directe d'utilisateurs réseau avec des demandes de bandes passantes élevées (des serveurs de virtualisation ou des systèmes de stockage ou d'archivage) via le port uplink.

AVoIP (Audio/Video over IP)

Sur le plan technique, Networked AV se base sur la norme IGMP et transforme des signaux HDMI en flux audio/vidéo transmis par des réseaux IP. Avec le « Dedicated Networked AV Mode », Zyxel intègre une technologie de forte demande dans des nombreuses séries switch de façon personnalisée et certifiée à l'aide de fabricants de composants audio et vidéo de renom tels que « Lumens », « ATEN » et « WyreStorm ». Le tableau de bord AV spécialement élaboré offre une surface web à utiliser de manière intuitive avec des fonctions Networked AV sélectionnées. Le menu fonctions supporte les utilisateurs lors de la configuration et la maintenance.

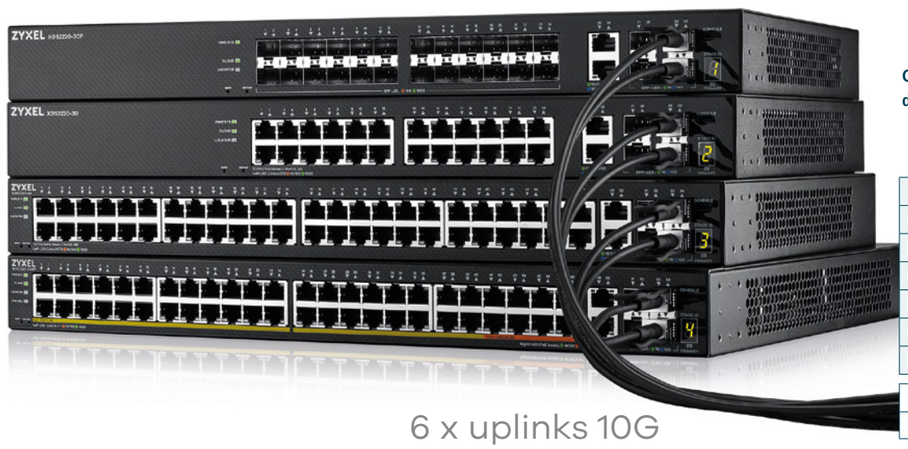
De l'empilement physique*
Des stacks physiques allant à quatre switch par stack seront disponibles comme dans la série précédente. Les avantages qui en résultent comme des connexions redondantes et une bande passante améliorée sont impératifs dans des environnements avec des hautes demandes de disponibilité.
** Disponible avec la prochaine version du firmware prévue pour août 2023*

Gestion facile et flexible avec NebulaFlex Pro
La série XGS2220 supporte la technologie Nebula-Flex Pro. Cela vous laisse la liberté de décider si vous voulez utiliser les appareils en mode autonome ou si vous voulez les intégrer dans notre plateforme de gestion cloud sans licence Nebula. La commutation entre les deux modes de gestion réseau est très facile. Zyxel continue de se concentrer sur la plateforme Nebula et rend de plus en plus de switch compatibles avec Nebula. La plus grande partie des switch administrables Zyxel sont déjà supportés par Nebula, à commencer par la série 1915.



Configuration et surveillance faciles avec le « Dedicated Networked AV Mode ».

Avantages pour les switch dans Nebula
Nebula permet de visualiser d'un coup d'œil l'occupation des ports. Le tout est représenté de manière encore plus spécifique avec des couleurs différentes correspondant à la vitesse de connexion de l'infrastructure connectée. Des icônes différentes permettent de voir immédiatement quels ports disposent de PoE, quel port agit en tant qu'uplink ou s'il y a un blocage « Spanning Tree Protocol » en raison de connexions parallèles avec une formation de boucles. Le tableau de bord est complété par une représentation chronologique de l'utilisation de la liaison montante, débit montant et descendant, ainsi que du budget PoE utilisé et disponible au maximum.



Comparaison des modèles de switch de la série Zyxel XGS2220

	XGS2220-30 (New)	XGS2220-30HP (New)	XGS2220-30F (New)	XGS2220-54 (New)	XGS2220-54HP (New)	XGS2220-54FP (New)
10G SFP+	4	4	4	4	4	4
Multi-Gigabit 10G Base-T	2	2	2	2	2	2
Ports Gigabit	24	24	–	48	48	48
Ports SFP	–	–	24	–	–	–
PoE 802.3at (30 watts)	–	16	–	–	40	40
PoE 802.3at (60 watts)	–	10	–	–	10	10
Budget PoE	–	400W	–	–	600W	960W
Référence	5276	5275	5274	5279	5278	5277
Prix	CHF 1'277.–	CHF 1'596.–	CHF 1'468.–	CHF 1'608.–	CHF 2'465.–	CHF 2'872.–

SÉCURITÉ

ZYXEL

Comment protéger le pare-feu des attaques

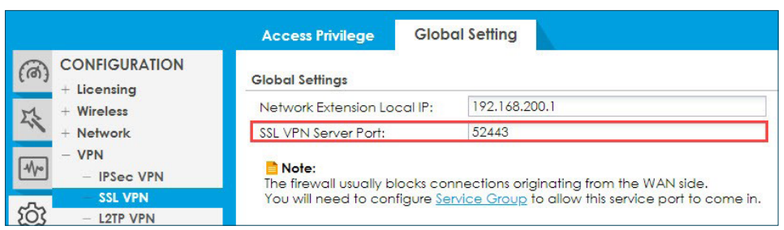
Le pare-feu est le premier obstacle pour des pirates sur Internet. Mais qu'est-ce qui se passe si le pare-feu est la cible d'attaques pirates et devient ainsi un risque potentiel ?

Un pare-feu protège le réseau local des accès non autorisés. Il est ainsi partie intégrante de tout concept de sécurité. En prenant des mesures de sécurité adéquates, le risque d'une attaque du pare-feu est minimisé. Tout d'abord, la personne responsable de l'administration IT devrait réfléchir qui a besoin d'accès au pare-feu d'où. Cela vaut pour des accès via Internet, pour des accès du réseau local ou via VPN. Dans beaucoup de cas, il suffit de limiter l'accès à quelques services pour des utilisateurs normaux, comme des consultations DNS sur le pare-feu ou le port pour la page d'avertissement des filtres de contenu. Seule la personne responsable de l'administration IT a besoin d'un accès à la console de gestion via SSH ou HTTP(S). Le mieux serait de limiter cet accès à quelques adresses IP dans les règles de pare-feu.

Accès de risque du WAN

Il faut accorder une attention particulière à la gestion à distance via le WAN. La solution la plus sûre serait bien entendu d'éviter complètement cette façon de gérer les pare-feux, mais dans la pratique, elle est une possibilité de gestion confortable. Si un tel accès est autorisé, il convient de respecter quelques points.

La solution la plus sûre est un accès via un VPN IPSec avec des paramètres de cryptage actuels, avec, idéalement, une authentification d'utilisateur supplémentaire. Cela permet de limiter en même temps l'accès admin à un seul utilisateur dans les règles de pare-feu, parce qu'il s'est déjà inscrit en mettant en place un tunnel au pare-feu. Cela est seulement possible lors d'un accès avec authentification précédente.



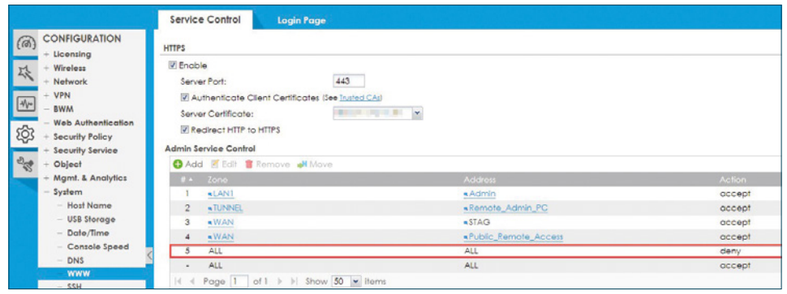
Au cas où le VPN SSL est utilisé, son utilisation est préférable avec un port spécial pour pouvoir repousser un balayage du réseau.

Le VPN SSL n'est pas recommandé, car il est basé sur la technologie SSL sensible. Si l'on envisage néanmoins de le faire, il faut au moins changer le port et l'accès à certaines adresses. Des objets FQDN (p. ex. des noms DynDNS) ou certaines adresses IP conviennent pour cela. GeoIP protège peu parce que des attaques sont réalisées aussi de la région autorisée et le lieu de provenance d'une connexion peut être caché facilement.

Dans les paramètres « HTTPS Service Control » peut être indiqué si une adresse IP a le droit d'utiliser le service seulement pour une connexion VPN SSL ou si elle a aussi l'accès admin.

De plus, il est possible que le pare-feu demande un certificat lors de la connexion avec le pare-feu via HTTPS ou VPN SSL. Dans ce but, un certificat racine de confiance peut être installé sur le pare-feu. Dans les paramètres WWW en revanche, l'option « Authenticate Client Certificates » est exigée. Ensuite, seul les clients qui disposent d'un certificat personnel authentifié par l'organe de certification correspondant peuvent se connecter.

Les conditions sont les mêmes pour la gestion à distance via HTTPS que pour le VPN SSL. Il est conseillé également ici d'utiliser un port alternatif qui diffère du port VPN SSL et de limiter l'accès à une adresse IP ou à un objet FQDN.



Le plus grand nombre d'accès doivent être bloqués.

Outre le HTTP(S), il y a d'autres services de gestion à distance tels que Telnet, SSH, FTP ou SNMP. Si ces services ne sont pas utilisés, ils peuvent être désactivés. Comme méthode alternative à SSH ou Telnet, il est possible d'utiliser la console web. Cette interface CLI peut être lancée via l'interface web dans le navigateur de façon conviviale.

L'authentification à double facteur

Les pare-feux Zyxel offrent également la possibilité de l'authentification à double facteur qui augmente la sécurité lors de la connexion de certains utilisateurs. Cette méthode est seulement possible pour les utilisateurs configurés pour cette authentification. Cela a pour conséquence que cette fonction peut être contournée dans quelques conditions. Néanmoins, son implication est tout à fait judicieuse.

L'ADP (Anomaly Detection and Prevention) protège le pare-feu en arrière-plan et repousse des anomalies tels que des scans de ports. Cette fonction peut contribuer à décharger le pare-feu en rejetant des paquets avant de les analyser de nouveau. Il est raisonnable d'activer l'ADP sur l'interface WAN.

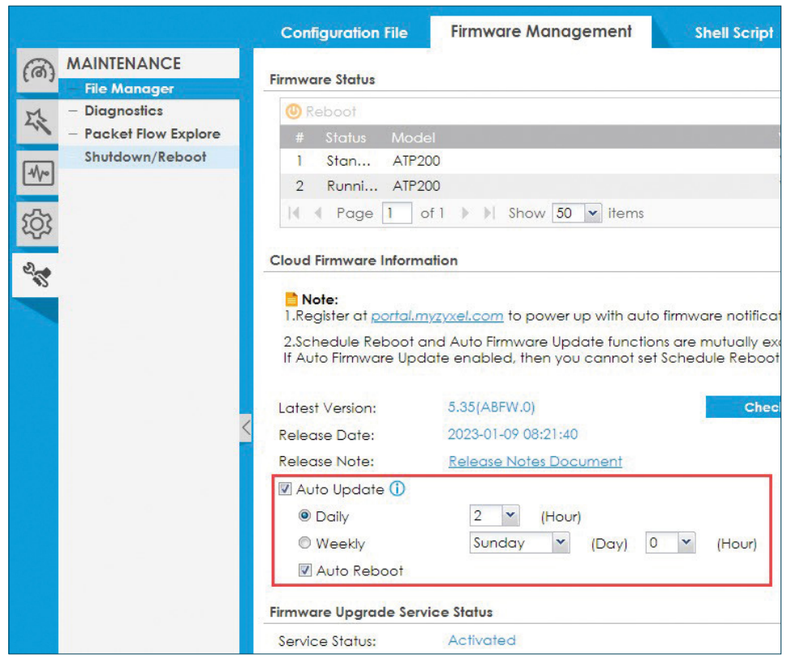
Des mises à jour de firmware importantes

L'essentiel pour terminer : mettez à jour votre pare-feu. Zyxel a renforcé les systèmes avec les dernières versions de firmware et peut ainsi réagir plus vite aux lacunes de sécurité. Pour des systèmes qui ne sont pas surveillés régulièrement, une mise à jour de firmware automatique est conseillée.

Pour certaines options, il peut avoir du sens de paramétrer un Alert Log qui déclenche tout de suite une alerte e-mail lors d'un évènement choisi. Cette fonction s'avère utile par exemple si un administrateur se connecte, notamment pour des pare-feux surveillés à intervalles irréguliers.

En résumé, on peut dire que des services hors service ne représentent aucun danger. Moins il y a des droits d'accès au pare-feu, plus sûre est le système.

L'entrée KB avec plus de détails sur la protection de votre pare-feu : **www.studerus.ch/kb-3823**



Une mise à jour de firmware automatique est conseillée.

SÉCURITÉ

ZYXEL

Bien configurer le pare-feu

Un pare-feu offre un grand nombre de fonctions qui protègent un réseau et des systèmes d'attaques. Ci-dessous les avantages et les désavantages de six fonctions importantes.

Voici un aperçu de quelques fonctions importantes d'un pare-feu. Nous vous conseillons de vous familiariser avec le sujet de sécurité avec une formation solide, par exemple avec des cours. Il y a les fonctions suivantes, à choisir selon vos exigences en matière de sécurité et l'effort que vous souhaitez déployer pour la configuration et l'entretien d'un pare-feu.

Bloquer des URL indésirables

Le service payant d'un filtre web ou d'un filtre de contenu pour des pare-feux apporte probablement la plus grande utilité de tous les services UTM. Des attaques typiques via des liens URL dans des e-mails sont bloquées par ces services. Il est conseillé de bloquer en général des URL inconnues.

⊕ Permet la restriction de l'accès aux sites web indésirables ou dangereux tels que des sites de phishing, des distributeurs de malware ou des contenus inappropriés.
- Une influence minimale sur la performance.
- De l'aide à la conformité aux directives de l'entreprise ou des exigences légales.
- Une augmentation de la productivité par le blocage des sites indésirables.

⊖ Des sites web pas encore catégorisés sont bloqués involontairement.
- Un contournement possible du blocage en utilisant des proxys ou des VPN.
- Une charge administrative augmentée pour le maintien et la mise à jour des URL bloquées.

Activer les services UTM

Les pare-feux ATP Zyxel offrent dans leur pack de service toujours tous les services UTM. Pour les USG FLEX, plusieurs packs sont disponibles selon besoin.

⊕ Une solution pour plusieurs fonctions de sécurité tels que le filtrage de contenu, le blocage d'URL, le filtre de réputation, l'anti-virus, l'anti-spam et la prévention d'intrusion.
- De la sécurité augmentée par l'utilisation de plusieurs mécanismes de protection dans une seule solution.
- Une gestion simplifiée par l'utilisation d'une seule console pour la gestion de toutes les fonctions de sécurité.

⊖ Un effort de calcul augmenté par le traitement de plusieurs fonctions de sécurité.
- Des éventuels problèmes de compatibilité avec quelques infrastructures ou de protocoles de réseau.
- Des éventuels contournements de fonctions de sécurité par des pirates expérimentés.
- Une charge administrative augmentée pour le maintien et la mise à jour des fonctions de sécurité intégrées.

Le LAN pas généralement ouvert vers le WAN

Dans la configuration de base, du trafic du LAN vers le WAN est en général permis. Du point de vue de la sécurité, il est conseillé de bloquer des connexions pas nécessaires.

⊕ Ainsi, du malware ne peut pas établir aisément des connexions Internet indésirables.
- Des restrictions dans le trafic via un pare-feu apportent en général plus de sécurité.

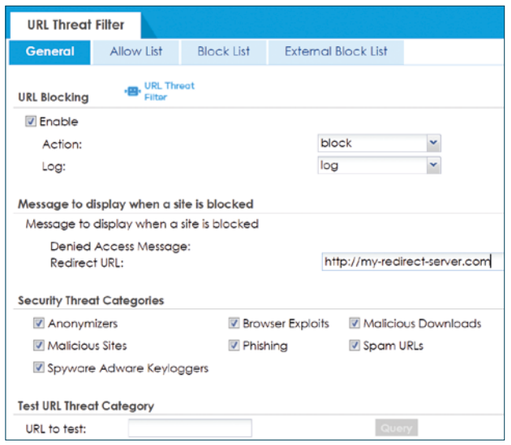
⊖ Une configuration supplémentaire est nécessaire.
- Pour surfer sur Internet, les ports 80 et 443 doivent être ouverts et peuvent être abusés pour des connexions indésirables.
- Une charge administrative augmentée pour le maintien et la mise à jour des règles du pare-feu.

L'nspection SSL

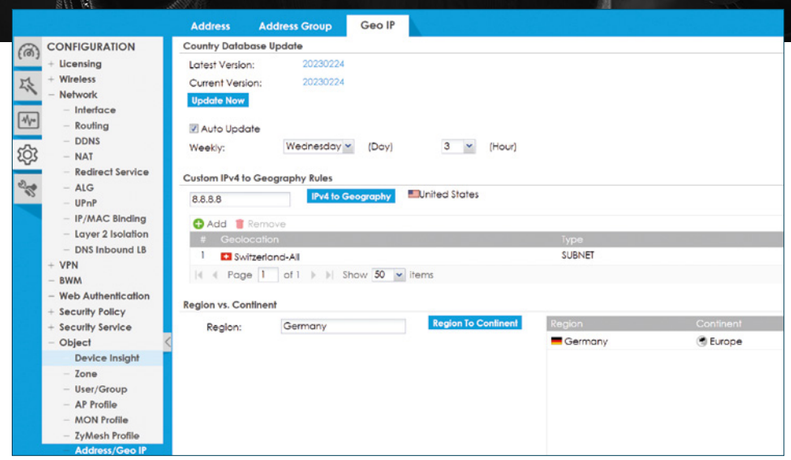
Cette fonction permet de détecter et de bloquer du malware et des attaques qui se cachent dans des connexions cryptées. Le plus grand nombre du trafic web et e-mail est chiffré avec du SSL et à peine accessible pour un pare-feu sans inspection SSL.

⊕ De la surveillance et du contrôle du trafic de données, même s'il est crypté.
- De la prévention des fuites de données par la surveillance des connexions SSL vers des ressources externes.

⊖ Un effort de calcul augmenté par du déchiffrement et du chiffrement du trafic.
- Des éventuels latences dans le trafic réseau à cause des étapes de traitement supplémentaires.
- Des éventuels problèmes de compatibilité avec quelques implémentations SSL.
- Un contournement possible de l'inspection SSL en utilisant du VPN.



Il est conseillé de bloquer toutes les Security Threat Categories.
C'est la protection la plus efficace contre une attaque de ransomware.



Geo IP permet de bloquer des accès indésirables de manière facile. Qui travaille qu'au niveau local devrait prendre cette précaution.

Geo IP

Le filtre Geo IP bloque des demandes du pare-feu sur la base du pays d'origine.

⊕ Pas de coûts supplémentaires (sans licence).
- Empêcher l'accès depuis des régions définies au réseau ou aux certaines ressources.
- Le trafic est rejeté en premier lieu et ne charge pas le pare-feu avec d'autres contrôles.

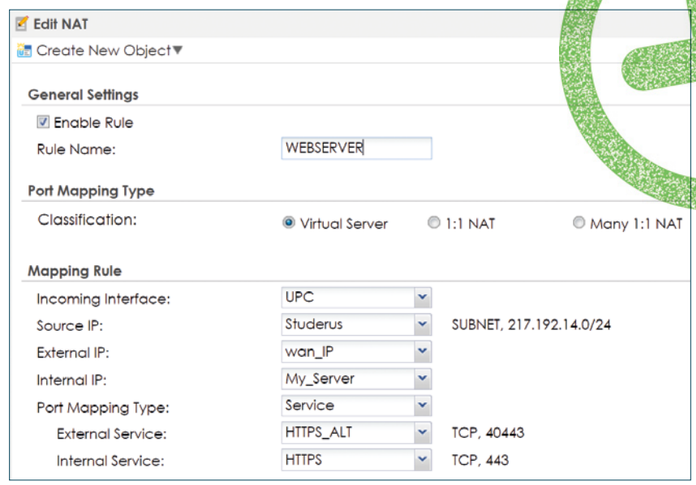
⊖ De la sécurité faible, le pays d'origine peut être facilement simulé (VPN).
- Une éventuelle coupure de l'accès pour des utilisateurs ou des applications légitimes.
- Une charge administrative augmentée pour le maintien et la mise à jour des adresses IP bloquées.

Le NAT : redirection de port

La redirection de port permet aux utilisateurs en dehors du réseau d'accéder aux ressources internes tels que des serveurs ou des applications. Configuré correctement, la sécurité est garantie.

⊕ La redirection de port peut faciliter la configuration du réseau en bloquant des connexions pas nécessaires aux ressources internes et en permettant seulement les connexions nécessaires.
- L'accès à la règle NAT peut être limité avec une IP source spécifique.
- Pour renforcer la sécurité, il est possible d'adapter le port externe à un autre port non courant.

⊖ La redirection de port peut présenter un risque de sécurité, car il permet l'accès aux ressources internes aux utilisateurs externes. Cela peut rendre possible l'accès des pirates à des données et des systèmes sensibles.
- Une redirection de port incontrôlée peut mener à une surcharge du réseau.



L'accès à un serveur interne doit être effectué avec d'éventuelles mesures de sécurité.

SUCCESS-STORY

ZYXEL

E-Quadrat net & media solutions

Comment devenir un fournisseur de services gérés

Le thème des fournisseurs de services gérés (MSP) continue de gagner du terrain, aussi dans les PME. Le partenaire Zyxel Gold E-Quadrat a mis en œuvre cette transformation avec succès. Lisez l'interview avec le propriétaire Jürg Stocker pour apprendre comment ils ont réussi.

Jürg Stocker, pourquoi voulais-tu devenir un Managed Service Provider (MSP) ?
Jürg Stocker : J'ai constaté que de plus en plus de fabricants et de sociétés fournisseur offrent leurs licences et leurs produits dans un modèle d'abonnement. Ce développement nous a également amené à réfléchir aux tâches et prestations que nous pourrions transformer en services.

En premier lieu, nous avons commencé d'offrir toutes les licences Office de notre clientèle via Office365 dans le modèle de location. Un an plus tard, nous avons ajouté une solution centrale de protection anti-virus et de sauvegarde en ligne. Nos nouvelles offres de service sont désormais les pare-feux, les switch et les points d'accès Zyxel via Nebula. C'est ainsi que nous sommes devenus un fournisseur de services.

Jürg Stocker
Propriétaire

Fournisseur informatique / partenaire
En 1999, Jürg Stocker a fondé l'entreprise E-Quadrat Sàrl. Le fournisseur de Rapperswil emploie aujourd'hui cinq personnes et conseille des petites et moyennes entreprises autour de la TEI. Depuis 2018, E-Quadrat est un fournisseur de services gérés (MSP).

Plus d'infos sur le fournisseur informatique sur :
www.e-quadrat.ch

Jürg Stocker dans l'interview avec Andreas Schmid

Est-ce que votre entreprise de 5 personnes n'est pas trop petit pour être un MSP ?
Pas du tout. Cela facilite notre travail énormément. Nous enregistrons des licences et des services d'une multitude de fabricants et les distribuons à notre clientèle. Notre personnel ajoute des employé·e·s ou des ordinateurs et prend des licences Office, anti-virus, sauvegarde et distantes pour la clientèle existante. Tout cela sans procédures de commande compliquées, mais tout simplement via les portails fabricant. Ou alors ils installent un pare-feu ou un point d'accès supplémentaire et les registrent via Nebula avec une licence.

« Nous avons pu réduire considérablement nos efforts tout en augmentant notre chiffre d'affaires »

La transformation était-elle facile et quelles étaient les obstacles à franchir ?
Cette transformation était facile. Entre-temps, nous servons 98 % de la clientèle avec ces services gérés. Chaque client·e reçoit un décompte mensuel de tout service et toute licence et paie seulement ce qui a été utilisé effectivement. Ce décompte était notre plus grand problème : En tant que fournisseur de service, nous recevons de nos sociétés fournisseur une facture avec une seule position pour leurs produits. Au début, notre employée administrative s'est inscrite à chaque portail, a noté le nombre de licences et services par client·e et les a indiqués individuellement sur chaque facture. Cette marche a pris beaucoup de temps et était une grande source d'erreurs. Un autre problème étaient les informations détaillées pour notre clientèle. Le/la client·e final·e veut savoir qui utilise quel produit, et quelle licence est pour qui etc. Il fallait trouver une solution.

Quelle est la solution que vous offrez aujourd'hui ?
Nous avons osé faire le pas et nous avons élaboré un concept sur comment et où nous avons besoin de quelles données et informations. Après une dizaine de mois, nous avons mis en place notre système d'information d'importation :

Les données sont téléchargées des différents portails de façon complètement automatisée. L'employée administrative peut créer les décomptes mensuels de façon entièrement autonome en moins d'une heure. En même temps, toute information essentielle pour la facture est mise dans un PDF et envoyé à la clientèle.

Nous utilisons ce système depuis plus de deux ans. Ainsi, nous avons pu réduire considérablement nos efforts tout en augmentant notre chiffre d'affaires. Et la clientèle a un aperçu à tout moment grâce aux rapports. Notre solution n'était bien entendu pas gratuite, mais nous avons déjà récupéré ces investissements.

Lisez ici **l'interview complète :**
www.studerus.ch/msp

APPEL !

Si vous souhaitez également devenir MSP, réservez une **démo web Nebula** d'une demi-heure avec Brice Baizez.
www.studerus.ch/fr/studerus-web-demos

POINT.