FleXos : Présentation Zscaler#

FleXos

| Z.I de Pt-Rechain | 4800 Verviers |
| Belgique | Tel. +32 87 293 770 |
| info@flexos.com |

| 31bis, rue Asdrubal | 1002 Tunis |
| Tunisie | Tel. +216 71 801 885 |
| info.tunisie@flexos.com |

| Euronext Bruxelles : FLEX |

Sommaire

1 La société FleXos

Fondée en 1991 et cotée sur le Marché Libre d'Euronext Brussels depuis le 5 mai 2008, FleXos est une société informatique belge active dans le domaine de la sécurité et du contrôle du réseau informatique. Elle propose ses services au niveau de l'audit et de la consultance sécurité et elle implémente des solutions de sécurisation des réseaux ICT. Une des ses principales missions est de conseiller les sociétés quant à l'utilisation de technologies novatrices qui permettent de combattre les nouvelles menaces plus efficacement et plus facilement.

FleXos consacre toute son énergie, son expérience et son savoir-faire à l'anticipation des besoins des entreprises en matière de sécurité et offrir ainsi à ses clients un service à haute valeur ajoutée. FleXos est de plus en plus reconnue pour son rôle de pionnier.

La mission de FleXos est d'identifier les enjeux face aux risques encourus en fonction des besoins identifiés:

- Mesurer le risque
- Développer une politique
- Appliquer les mesures de protection
- Maintenir le niveau de sécurité

2 FleXos Security-as-a-Service

Prenez l'avantage dans la lutte contre les logiciels espions, les virus Web et les usurpations d'identité grâce à la sécurité externalisée. Bloquant les menaces et les contenus non désirés avant qu'ils n'atteignent votre réseau, nous éliminons les couts d'achat, de maintenance, de support et de mise à jour de votre infrastructure réseau, vous permettant de vous concentrer sur vos projets IT les plus cruciaux.

Pourquoi passer à la sécurité externalisée

Zscaler a une plus grande visibilité sur le trafic Web que les autres solutions existant actuellement sur le marché. Les données sont traitées en temps réel, ce qui permet d'identifier de nouvelles menaces plus rapidement et plus efficacement. Nos clients sont totalement protégés sans avoir à télécharger de mise à jour.

Avec Zscaler, vous bénéficiez de la meilleure solution du marché en matière de protection incluant:

- Sécurité Web & Email avancée (antivirus/antispyware, antispam, menaces nouvelles génération)
- Sécurité des navigateurs
- Filtrage d'URL
- Contrôle du Web 2.0
- Gestion de la bande passante
- Prévention contre la fuite d'information

FleXos est actuellement implanté en Belgique, au Luxembourg, en Tunisie et en Algérie.

Belgique & Luxembourg

FleXos ICT Belgium SA
Z.I. de Petit-Rechain
4800 Verviers
Belgique
Tél. +32 (0)87 293 770
Fax. +32 (0)87 231 509
Email. info@flexos.com

Tunisie, Algérie & Afrique

FleXos Tunisie SARL
31bis, rue Asdrubal
1002 Tunis
Tunisie
Tél. +216 71 801 885
Fax. +216 71 801 575
Email. info.tunisie@flexos.com

Un simple changement de configuration redirige votre trafic vers nos centres opérationnels. Votre trafic est alors scanné en temps réel, en tenant compte de vos politiques d'utilisation et en bloquant les virus Web, logiciels espions, chevaux de Troie, usurpations d'identité, menaces venant des Messageries Instantanées et contenus inappropriés avant qu'ils n'atteignent votre réseau.

FleXos sélectionne ces partenaires selon des critères technologiques, et par le niveau d'implication des éditeurs à satisfaire nos clients. Zscaler a été désigné comme l'acteur le plus visionnaire dans le Gartner Magic Quadrant dans la catégorie passerelle de sécurité Web.

Les avantages

- Sécurité Inégalée - une réelle protection multi-niveaux grâce aux moteurs se basant sur des signatures et au propre moteur heuristique
- Coût Total de Possession très faible - Nos clients constatent généralement une réduction de 30 à 40% de leurs coûts total de possession (TCO)
- Facilité de Déploiement - La sécurité Web externalisée est conçue pour un déploiement facile et souple permettant une gestion granulaire (par utilisateur)
- Evolutivité Instantanée - Notre suite de services managés peut être adaptée à l'infini, vous permettant d'ajouter des utilisateurs instantanément à un coût fixe
- Accords de qualité de service inégalé (SLAs) - Nous vous garantissons une disponibilité de nos services de 99,99 %
- "Zero" Latence - Notre service a été conçu spécialement pour le trafic Web afin que vous ne ressentiez aucune perte de vitesse

3 Les nouveaux défis

Ces dernières années l'utilisation du Web dans les entreprises s'est généralisée. Notamment grâce aux nouvelles technologies qui permettent d'associer au Web des fonctions transactionnelles et visuelles avancées. Les applications métiers se sont ainsi converties au Web soit par une migration technologique sur le réseau de l'entreprise soit par une souscription à une offre de service sur Internet. Ainsi le navigateur est devenu indispensable et est bien souvent le principal outil de travail. Il se retrouve donc naturellement au centre des convoitises et on constate aujourd'hui que la grande majorité des menaces ciblent l'utilisation et le contrôle de nos navigateurs. Malheureusement peu d'outils réellement efficaces ont été déployés pour en sécuriser et contrôler l'usage. Ces nouvelles malveillances posent de réels défis aux Responsables de Sécurité des Systèmes d'information (RSSI) des entreprises, qu'il s'agisse de réseaux de zombies ou bots, de phishing ou de failles de sécurité en évolution constante liées à des contenus actifs (Flash, JavaScript…) et malicieux (exemples : Cross Site Scripting ou XSS, Cross-Site Request Forgery ou CSRF, Clickjacking, vol de cookie,…).

D'autre part, le phénomène des nouveaux sites « Web 2.0 », réseaux sociaux, Peer-to-Peer, vidéo, etc… créent à la fois e nouvelles opportunités et des risques pour l'entreprise. Ces applications aident, par exemple, à développer des communautés d'intérêt pour le marketing, mais peuvent aussi générer des pertes de productivité, l'utilisation abusive des ressources (bande passante), des risques de responsabilité légale ou de fuite d'informations confidentielles, et puis toujours le risque pour les utilisateurs de télécharger des données malicieuses. Egalement, l'utilisation de plus en plus croissante d'Internet en situation de mobilité, notamment à travers des Smartphones, amplifie ce phénomène, d'autant plus que leurs accès à Internet ne sont le plus souvent pas soumis aux contrôles de sécurité de l'entreprise.

Les solutions actuellement disponibles sur le marché posent plusieurs types de contraintes et de limitations: d'abord elles sont coûteuses à la fois en acquisition et en maintenance et administration; elles sont complexes à déployer et à gérer puisqu'il s'agit d'accumuler dans la DMZ des serveurs pour les rôles de Proxy, d'URL Filtering, d'anti-virus & Anti-spyware, ... serveurs qu'il faut maintenir, faire évoluer, mettre à jour,…

Ensuite, elles montrent vite leurs limites parce que les anti-spyware ne sont plus suffisants, et parce que les politiques d'usage s'appuient essentiellement sur les URL pour autoriser ou pas l'accès à certains contenus. Or avec le Web 2.0 l'URL n'est désormais plus un critère suffisant, puisque des contenus de nature pour le moins controversée se retrouvent dans des sites variés. Selon les analystes du marché, environ 75% des malware se retrouvent dans des pages Web sur des sites légitimes, ayant une bonne réputation. Par ailleurs, ces solutions prennent très mal en compte les bureaux à distance et les utilisateurs mobiles, et enfin elles ne fournissent que du reporting orienté vers les serveurs en question, mais pas de visibilité consolidée et multicritère sur l'ensemble des flux HTTP de l'entreprise.

4 L'approche Saas

Afin de répondre à ces problématiques, Zscaler fournit une solution en mode Saas, complète, transparente et très facile à mettre en œuvre, pour pallier ces nouveaux risques. Zscaler propose aux entreprises d'éliminer la complexité et les coûts mentionnés ci-dessus, et de les transférer à Zscaler.

Zscaler a déployé un Cloud au niveau mondial, avec des points de présence dans les principales métropoles des grandes plaques régionales. Pour bénéficier du service, il suffit pour l'entreprise de rediriger le trafic Web, à la sortie du Firewall ou du routeur, vers le point d'accès le plus proche de l'infrastructure de Zscaler. Le trafic de chaque utilisateur vers Internet est alors filtré à très haute vitesse, puis autorisé, bloqué ou régulé, en fonction de la politique de filtrage définie par l'entreprise pour cet utilisateur. Au retour, Zscaler analyse le contenu Web pour détecter les menaces malveillantes et délivrer un trafic nettoyé à l'utilisateur afin de protéger ce dernier lorsqu'il accède aux ressources Internet.

Le résultat est de permettre aux entreprises de regagner le contrôle et la visibilité des flux HTTP et HTTPS, et ainsi de limiter les abus et de « contrôler plutôt que d'interdire ».

La solution Saas de Zscaler élimine les coûts d'acquisition des produits de sécurité, les coûts de déploiement et les coûts de maintenance. Les entreprises paient uniquement une souscription annuelle pour utiliser le service en fonction du nombre d'utilisateurs.

En ce qui concerne leurs sites distants, beaucoup de grandes entreprises ont opté pour une architecture centralisée, forçant les utilisateurs à distance à passer par une passerelle unique en central, même pour surfer sur Internet, via le réseau interne d'entreprise ou un accès VPN. Ceci a été décidé parce qu'à l'époque c'était la seule manière d'assurer la sécurité et le contrôle de ces flux, mais cela provoque des lenteurs difficilement supportables, et génère des coûts télécom énormes qui pourraient facilement être évités.

D'autres ont choisi une architecture décentralisée, avec de multiples passerelles Internet distantes, mais alors ceci implique normalement de multiplier les produits de sécurité Web.

Zscaler permet de briser ce paradoxe, c'est-à-dire de laisser les utilisateurs distants avoir accès à Internet localement, de manière à la fois rapide et bon marché, tout en augmentant le niveau de sécurité global de l'entreprise, et en fournissant un contrôle et une visibilité améliorés. Le trafic de chaque bureau distant ou de chaque utilisateur mobile est redirigé vers le même Cloud filtrant, en son point d'accès le plus proche, et ainsi la même politique s'applique à un utilisateur donné, quelle que soit sa localisation.

5 Zscaler Web Security Cloud

La solution Zscaler comporte quatre grands ensembles de fonctionnalités : « Secure » (sécurité), « Manage » (gestion des droits et ressources), « Comply » (inspection des contenus), et « Analyze » (analyse des logs et le reporting).

Zscaler fournit un service complet d'analyse « in the Cloud » prévenant des risques tout en simplifiant l'administration IT. La technologie de Nanolog assure une performance de l'activité Web en temps réel. Utilisant des technologies avancées (ByteScan, PageRisk) combinées aux plateformes proxy de haute performance, le service assure une sécurité optimale sans dégradation des performances.

Sécurité Web avancée

Anti-virus & anti-spyware : Mises à jour en temps réel des moteurs de signatures et d'analyses dynamiques pour une protection totale contre les virus et spyware. Les entreprises et utilisateurs nomades sont désormais protégés sans risque d'exposition.

Menaces nouvelles génération : Le Research Center 24x7 identifie et bloque les nouvelles menaces tel que les contenu malicieux, botnets, cross site scripting (XSS), cross site request forgecy (CSRF), phishing et les nouveaux pièges du Web 2.0.

Sécurité des navigateurs : Les browsers obsolètes représente une faille de sécurité dans l'environnement de l'entreprise. Web Security Cloud vérifie que votre navigateur est à jour avant que les utilisateurs accèdent à Internet. Zscaler fournit un bouclier protégeant des attaques lorsque les internautes utilisent un navigateur ou plugin vulnérable.

Gestion des accès Internet

Filtrage d'URL : Une combinaison de moteurs puissant de classification et une équipe humaine basée sur cinq continents catégorisent des millions d'URL. Cependant, l'analyse traditionnelle n'est pas suffisante. La technologie Dynamic Content Classification analyse les pages lors de leurs accès et fournit ainsi un second niveau de protection en temps réel. Bien entendu, Zscaler classifie les contenus avant que les pages soient protégées par un mot de passe.

Contrôle Web 2.0 : Bloquer tous les sites Web 2.0 n'est pas pratique. Les entreprises ont besoin d'autoriser certains, mais de filtrer les contenus malicieux se propageant très rapidement en environnement Web 2.0. Les moteurs de scan haute performance analyse des milliers de sites Web 2.0. Ainsi les contenu malicieux sont identifiés et immédiatement bloquer au niveau d'Internet.

Contrôle de la bande passante : La consommation de la bande passante explose. La vidéo consomme vingt fois plus de bande passante que les données traditionnelles. Web Security Cloud permet aux sociétés de contrôler qui consomme, combien de bande passante, à quel moment de la journée, depuis quel endroit, ceci permet d'améliorer à la productivité à moindre coût.

Prévention contre la fuite d'information et services de conformité

Dictionnaires : Zscaler fournit des dictionnaires pouvant détecter trois types de données : nombre défini (Carte de crédit, SSN, Canadian SIN, …) sur lequel un contrôle est effectué pour éviter la génération de faux positifs; détection de document (financier, médical, code source,…) via un moteur doté d'une intelligence artificielle ; phrases paramétrables que l'administrateur intègre afin que le système détecte tout document ou conversation quittant l'organisation utilisant les termes.

Data Leakage Engines : Les dictionnaires sont combinés à des moteurs détectant et bloquant les transactions afin d'être conforme aux normes PCI ou HIPPA. En complément, l'administrateur peut définir une relation entre les moteurs et ses propres dictionnaires afin de bloquer la violation de la propriété intellectuelle.

Applications : Zscaler scanne toutes les données sortantes de l'organisation à travers toutes les applications Web. Les moteurs analyses tous les documents en format Microsoft, PDF ou compressés. Les règles granulaires peuvent s'appliquer à des utilisateurs, des sites ou selon des applications spécifiques tels que les réseaux sociaux, webmail ou messagerie instantanée.

Consolide et simplifie la sécurité Web des entreprises

- Sécurité avancée pour le Web 2.0 automatiquement mises à jour contre les dernières menaces sans intervention des ressources IT internes
- Huit modules totalement intégré pour couvrir les risques en sécurité, responsabilité et fuite de données
- Reporting et accès aux logs en temps réel, le service IT libéré des tâches sans valeur ajoutée

Latence négligeable pour tous les employés, équipements, partout dans le monde

- La plus grande infrastructure « in the Cloud » déployée dans le monde, plus de 40 Datacenter pour répondre aux besoins de clients à travers plus de 140 pays
- Infrastructure locale, nationale et intercontinentale redondante et hautement disponible
- Accessibilité totale pour l'utilisateur, n'importe quel utilisateur peut se connecter à n'importe quel Datacenter et navigue en toute sécurité sur Internet

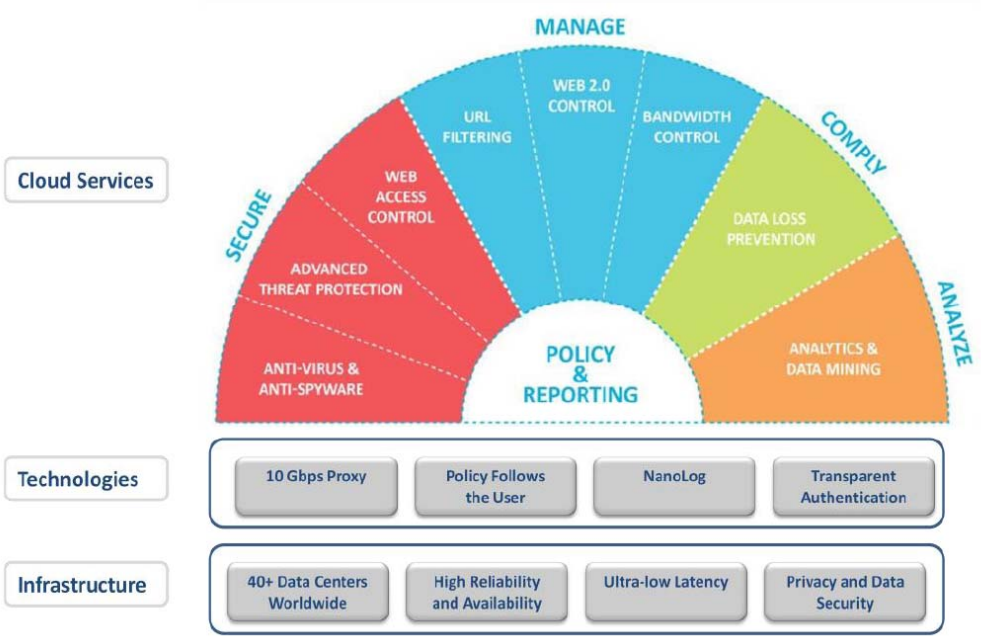
Réduction des coûts

- Pas d'acquisition d'appliances, de logiciels, de clients poste de travail
- Aucune dépense d'investissement, faible TCO
- Pas de coût de sur capacité, payer juste en fonction de vos besoins
- Une souscription pour couvrir les besoins de tous les bureaux et utilisateurs nomades

Rester à la pointe de la technologie

- Sécuriser les nomades n'est pas une option, mais une nécessité. Zscaler couvre tous les utilisateurs dans le monde
- Cloud ne signifie pas latence. L'infrastructure Zscaler fournit une protection sans failles et sans délais.
- Garder le contrôle de votre politique et de la gestion de vos logs. Les « Nanolog » confèrent un accès permanent à tous les traces à travers le monde

Zscaler_Une infrastructure mondiale hautement disponible



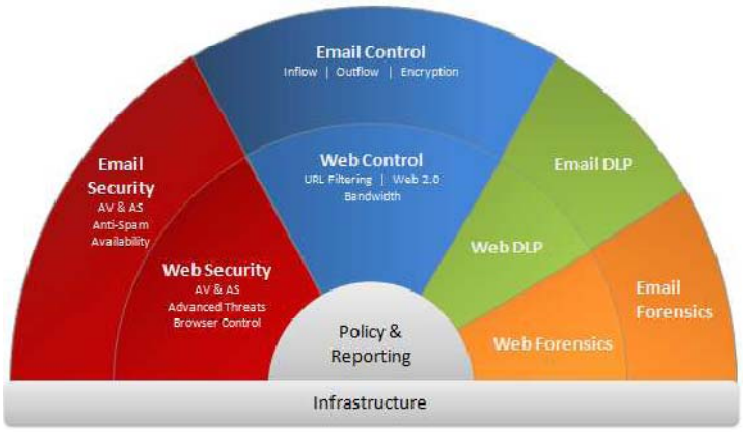
Zscaler_Un éventail de fonctionnalités

6 Zscaler Email Security Cloud

Compte tenu de la croissance exponentielle du spam et de la complexité des moyens à mettre en œuvre pour garder le contrôle, les entreprises ont rapidement adoptées les solutions de sécurité Email basées sur le Cloud Computing. Elles bénéficient ainsi d'une évolution illimitée, d'une sécurité accrue, d'une optimisation des ressources tout en optimisant les coûts. Zscaler est le premier acteur à proposer une solution Saas intégrant une protection contre les virus et malware, contrôle des flux et une prévention contre la fuite d'information. Cette approche permet une synchronisation LDAP simplifiée, une gestion unifiée des politiques, un reporting centralisé concernant aussi les besoins Email que Web à travers une infrastructure mondiale.

Politique et reporting unifiés Email & Web

Les administrateurs disposent d'une console unique pour définir les politiques de sécurité, d'anti-spam, gestion des flux Email et DLP. Les responsable IT gèrent leurs propres politiques et chaque changement est répliqué sur l'ensemble de l'infrastructure Cloud instantanément. Les logs peuvent être consultés en temps réel quelque soit la localisation. Plus de 30 rapports sont prédéfinis auxquels s'ajoute la possibilité de drilldown assurent aux administrateurs l'accès aux logs détaillés.



Zscaler_Sécurité et contrôle Email & Web unifiée

Sécurité Email avancée

Anti-virus et Anti-Spyware : Les moteurs de signatures et d'analyse dynamique sont constamment mis à jour délais afin de protéger efficacement les entreprises contre les spyware et nouvelles variantes de virus.

Anti-Spam : Moteurs de réputation de classe mondiale associés la technologie anti-spam Zscaler permet de bloquer toutes les nouvelles menaces de type spam. Le moteur anti-spam intègre une détection d'images, d'URLs malicieuses et mutation en temps réel. Chaque utilisateur accède à sa zone de quarantaine à partir de laquelle il peut relâcher ou au contraire bloquer un email suspect.

Disponibilité : Zscaler simplifie les mesures de prévention inclus dans un plan de disaster recovery grâce à l'infrastructure maillée « in the Cloud ». Delivery Assurance : Zscaler conserve les messages dans le cas d'une indisponibilité du serveur de messagerie. DDoS Protection : Zscaler bloque les attaques de type denial of service sur le nuage avant même les réseaux des clients, libérant ainsi les serveurs de messagerie et pare-feux d'un trafic volumineux non sollicité. Le service prévient contre les directory harvest attack assurant ainsi une protection des serveurs et des informations.

Règles de gestion des flux Email

Entrant et sortant : A travers une politique simple et intuitive, Zscaler offre des règles granulaires concernant tous les messages transitant via le service selon le destinataire, l'émetteur et types de fichiers joints.

Alias et renommage : La gestion des alias, du routage d'Emails et de création de copies est simplifiée à travers la politique d'Alias et renommage. Les entreprises ayant plusieurs domaines de messagerie peuvent communiquer à l'extérieur qu'à partir d'une adresse unique.

Chiffrement : Zscaler s'assure que les messages sont délivrés à partir d'un MTA sécurisé. A partir de la combinaison émetteur / destinataire / contenu du message, l'administrateur peut exiger que l'email transitera via un canal chiffré.

Email DLP et services de conformité

Les utilisateurs peuvent accidentellement ou volontairement transmettre des données sensibles via leur compte de messagerie. Zscaler prévient du risque de divulgation d'information et par conséquent de la mise en cause de la responsabilité de l'entreprise en analysant tout le trafic sortant en fonction de règles paramétrables et prédéfinies tels que HIPPA ou PCI Compliance.

Dictionnaires : Tout comme le service Web, Zscaler fournit des dictionnaires contre la fuite d'information selon des combinaison de nombre, type de document, de mots et combinaison de mots clés paramétrables ainsi qu'à partir de moteur à l'intelligence artificielle. Ainsi, le systèmes détectera et bloquera les documents et conversations correspondantes.

Data Leakage Engines : La combinaison des dictionnaires et des moteurs DLP permet de se conformer aux normes HIPPA et PCI ainsi qu'à une politique interne de protection de la propriété intellectuelle.

Règles DLP : Le service Zscaler Email Security Cloud analyse tous les messages sortants de l'organisation incluant les corps du message, les attachements aussi bien en format

Microsoft, PDF, compressé. En fonction des règles, les messages chiffrés sont délivrés ou mis en quarantaine avec possibilité de notifications.

Consolide et simplifie la sécurité Email

- Console d'administration unique pour la définition des politique Email et Web
- Maillage technologique pour une protection renforcée et prévention des pertes de données
- Accès aux logs et reporting disponible en temps réel

Implémentation rapide

- Aucun équipement à installé, simplement pointer les enregistrements MX vers Zscaler
- Politique intuitive et granulaire pour une gestion simple des flux de messagerie
- Quarantaine utilisateurs accessible sans besoin de ressources internes

Réduction des coûts

- Pas d'acquisition de matériel et logiciel
- Pas de coûts d'investissement
- Modèle sous forme d'abonnement prévisible correspondant aux besoins réels
- Suppression des frais indirect grâce à une optimisation des ressources (bande passante, stockage, exploitation…)