

FleXos : Présentation Fortinet#



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	3
2	La société Fortinet	5
3	L'approche Fortinet.....	8
4	Portfolio.....	10
5	FortiGate	11
6	Les applications Fortinet.....	12
a.	Firewall.....	12
b.	IPS	13
c.	VPN-IPSec et SSL	14
d.	Inspection SSL.....	14
e.	Wireless	15
f.	Optimisation WAN.....	16
g.	Antivirus	16
h.	Antispam	17
i.	Web filtering	18
j.	Contrôle applicatif	18
k.	Web Application Security	19
l.	DLP	19
m.	Database Security.....	20

1 La société FleXos

Créée en 1991 et cotée sur le Marché Libre d'Euronext Brussels depuis le 5 mai 2008, FleXos est une société de services active dans les réseaux informatiques, les solutions de sécurité, l'assistance, conseil et intégration informatique.

FleXos est le partenaire privilégié et reconnu par les acteurs du marché. En plus de 15 ans, FleXos s'est ainsi forgé une solide réputation. Etre à l'écoute d'un monde en évolution constante, c'est anticiper les besoins de nos clients. Nous nous positionnons comme un véritable partenaire, ayant pour objectif de trouver ensemble des solutions informatiques fiables, flexibles ... indispensables à la croissance et aux performances de votre entreprise.

FleXos, c'est une équipe stable, dynamique, soudée et extrêmement flexible qui comprend les besoins des entreprises et administrations de toute taille aussi bien en Europe qu'en Afrique.

Janvier 2008 a vu l'implantation d'un bureau opérationnel à Tunis afin de servir de base à nos équipes d'ingénieurs pour couvrir le continent africain.

Notre partenariat étroit avec Fortinet (leader mondial des Firewalls UTM) nous autorise à vendre et à réaliser l'installation de matériel de sécurité Fortinet sur tout le continent africain. De plus, nous disposons d'un centre de formation Fortinet à Tunis (en collaboration avec l'Université Centrale) nous permettant de former des personnes venant de toute l'Afrique sur les différents matériels Fortinet. FleXos est certifié Gold Partner Fortinet.

FleXos collabore aussi régulièrement avec des sociétés informatiques locales et les aide à répondre à des demandes pointues en sécurité informatique.

D'importants clients étiquetés "Défense", "Sécurité" ou "Gouvernement" sont gérés directement par FleXos avec la plus grande discrétion s'agissant de projet ayant trait à la "Sécurité d'Etat" afin d'assurer le respect des "normes" Internet propres à chaque pays.

A sa demande, chaque prospect ou client peut être visité dans son pays. Chez FleXos, nous sommes très réactifs quand il s'agit de projets liés à la sécurité.

Toute réponse technologique est le fruit d'une vraie rencontre, d'une réflexion ... et d'une approche humaine.

Vous êtes unique. La gestion d'une infrastructure informatique (installation, réseau, sécurité, ...) nécessite, par conséquent, un dialogue ouvert et constructif pour définir, avec un maximum d'exactitude, les besoins réels de votre entreprise.

Nos audits sont réalisés dans la plus grande confidentialité.

En prenant en charge les problèmes informatiques de façon globale et complète, nous permettons à l'entreprise de se consacrer essentiellement à ses objectifs commerciaux.

Le savoir-faire de notre équipe au niveau systèmes, réseaux, messageries, d'Internet, sauvegarde et de sécurité nous permet de garantir des interventions rapides et parfaitement fiables.

La sécurité informatique est un souci permanent. Nous proposons des systèmes de protection extrêmement efficaces contre les attaques et intrusions non-désirées. Firewalls,

anti-virus, contrôle e-mail, analyse en temps réel des fichiers téléchargés, analyse du flux Internet, accès sécurisés pour accès à distance (VPN), contrôle de l'accès Internet aux sites "non productifs" ou répréhensibles, ...

Nous pouvons aussi auditer votre système et dresser un état de la sécurité de votre réseau informatique grâce à notre solution analysant des milliers de vulnérabilités en temps réel.

En partenariat avec nos organismes financiers dont BNP Paribas, nous assurons le financement (leasing) de vos acquisitions.

Pour nos clients, nous sélectionnons nos fournisseurs pour la qualité de leurs produits et l'efficacité de leurs services.

Dans le cadre de nos projets chez nos clients, nous travaillons avec Microsoft, HP, Zscaler, Fortinet, Trend Micro, Fortinet, Citrix, VMware, Blackberry, ...

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

2 La société Fortinet

Fortinet est un acteur mondial de la sécurité réseau à travers une gamme d'appliances et leader sur le secteur des UTM (Unified Threat Management). Les produits et services fournissent une protection complète, intégrée et de haute performance contre les nouvelles menaces tout en simplifiant l'infrastructure sécurité.

Nos clients sont aussi bien des entreprises, des opérateurs et entités gouvernementales de tous pays, incluant une majorité des sociétés classées dans le Fortune Global 100. Fortinet, coté au Nasdaq, est présent dans le monde entier.

La plateforme de sécurité FortiGate, le produit phare de Fortinet, offre une combinaison puissante basée sur une technologie ASIC propriétaire afin d'assurer une accélération des performances, des solutions intégrées de protection en profondeur contre les menaces multiples constamment mises à jour. A la pointe de l'innovation dans les domaines réseaux, sécurité et analyses de contenu, Fortinet intègre une large suite de technologies incluant les fonctionnalités de pare-feu, VPN, anti-virus, prévention d'intrusion (IPS), filtrage Web, anti-spam, gestion de trafic. Les modules peuvent être utilisés séparément ou combinés pour une gestion complète et unifiée des menaces. Fortinet complète cette gamme avec des solutions d'analyse, email, sécurité des bases de données et d'équipements d'utilisateurs finaux.

A ce jour, Fortinet a déployé plus de 500 000 appliances dans plus de 75 000 clients du monde entier.

Un point différenciateur important, les processeurs propriétaires d'analyse de contenu et réseau, FortiASIC, permettent aux systèmes FortiGate de détecter et supprimer des menaces complexes en temps réel sans dégrader les performances. La suite complète de gestion, d'analyse, de protection des postes et bases de données permet une flexibilité en termes de déploiement tout en se conformant aux règles émises par l'industrie et les gouvernements. Cette approche permet également de réduire les coûts d'acquisition et de gestion de gestion des infrastructures sécurité.

Les points forts :

Une technologie 100% propriétaire

- Maîtrise de l'interopérabilité des fonctionnalités.
- Indépendance juridique limitant les risques vis à vis des utilisateurs.
- Positionnement financier original: licence illimitée.

La performance de l'ASIC au bénéfice des fonctionnalités de sécurité

Excellent ratio prix / performance

Une logique de gamme attractive pour tout type d'utilisateurs

- Même niveau de sécurité pour un opérateur / un Grand Compte/ une Pme,
- Une flexibilité d'utilisation des fonctionnalités,
- Une évolutivité fonctionnelle (VPN SSL, Protection IM, ...),
- Une évolutivité en performance (clustering...),
- Une administration et reporting centralisé.

Les bénéfices de l'UTM et de la virtualisation : Réduction des coûts directs / Réduction des coûts indirects, tout en assurant un très haut niveau de sécurité et ceci à haut débit.

Plus de 700 Ingénieurs en recherche et développement réfléchissent tous les jours aux futures technologies de sécurité.

Analyses et certifications

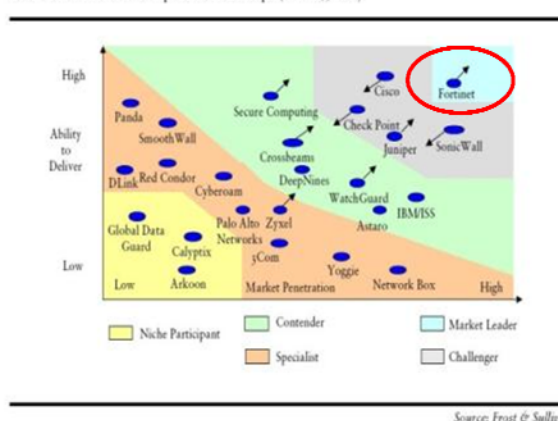
Depuis sa création en 2000, le positionnement de Fortinet a été reconnu par des cabinets d'études, des organisations indépendantes et les journalistes. Fortinet a reçu plus de 100 récompenses, tels que :

- Leader Mondial des UTM (IDC, Frost & Sullivan).
- Top 4 des vendeurs d'appliances de sécurité (IDC).
- Classé leader par le Gartner au niveau du Magic Quadrant des solutions firewall multifonction.
- Classé « Top Player » dans le Gartner MQ Email Security Appliance.
- Nommé « Network Security Vendor » de l'année 2010 par Frost & Sullivan.
- Vainqueur du trophée SC Magazine « Meilleure solution de sécurité intégrée » en 2009.
- Primé par le CRN Tech Innovateur de l'année 2009.



F R O S T & S U L L I V A N

Total UTM Market: Competitive Landscape (World), 2007



Source: Frost & Sullivan

Fortinet dispose de nombreuses certifications tels que

- 7 ICSA Security certifications.
- NSS UTM certification.
- ISO 9001 certification.
- 12 Virus Bulletin (VB) 100% awards (antispam, antivirus...).
- IPV6 certification and Common Criteria Evaluation Assurance Level 4 Augmented (EAL 4+) for FortiOS 3.0.

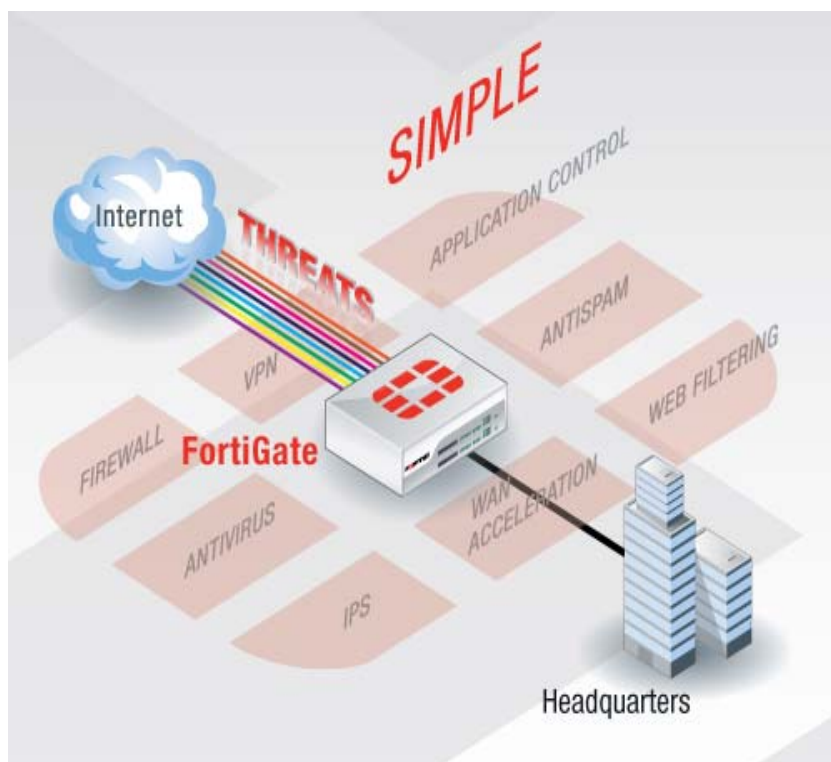


3 L'approche Fortinet

Fortinet s'est spécialisé sur le marché des UTM, équipements intégrant plusieurs fonctionnalités en une seule appliances associé à une console unique de management et reporting.

Cette approche procure plusieurs avantages, dont notamment :

- Optimiser des ressources.
- Technologie ASIC intégré pour des meilleures performances.
- Déploiements, administration et l'exploitation simplifiés.
- Réduire du nombre équipements hétérogènes.
- Réduction du nombre de « points de fêlures ».
- Modules de sécurité intégrés.
- Sécurité avancée en profondeur.
- Mises à jour automatiques et constante pour plusieurs fonctionnalités en une fois.
- Support unique.
- Mises à niveau des compétences IT simplifiées.
- Coût d'acquisition et maintenance réduit.
- Retour sur investissement rapide, coût total de possession réduit.



En termes de sécurité, cette approche permet d'avoir des analyses multi-niveaux complémentaires notamment au niveau de contenu des applications, l'ensemble étant intégré.

4 Portfolio

Les solutions complètes de sécurité Fortinet combinent de multiples technologies de sécurité évolutives et intégrées dont les organisations modernes ont besoin. Fortinet fournit la plus grande suite de sécurité accessible depuis une interface d'administration unique facilitant ainsi le déploiement et la gestion des politiques. Mises à jour automatiques et en temps réel des bases de données de protection délivrées par le centre de recherche des menaces FortiGuard® (Global Threat Research Team) permettent aux organisations d'être à la pointe de la protection contre les menaces en perpétuelles évolution. Afin d'obtenir le plus faible coût total de possession (TCO), la souscription est calculé par équipement pour un nombre illimité d'utilisateurs.

La gamme de passerelle de sécurité Fortinet offre des modules complémentaires basée sur le système ASIC pour des performances optimisées, une protection multi-niveau intégrée, constamment mis à jour, analyse intelligente et en profondeur des menaces. Cette combinaison unique délivre un très haut niveau de sécurité réseau, de contenu, applicatif pour les entreprises de toutes tailles, fournisseurs d'accès, opérateurs de service tout en réduisant le coût total de possession et offrant une évolution, une flexibilité en adéquation avec les futurs besoins.

Sécurité réseau



FortiGate
Plateforme de
sécurité réseau
Multi-menaces

Management



FortiManager
Management
centralisé
FortiAnalyzer
Gestions des logs
& génération de
rapports

Sécurité des données



FortiDB
Sécurité des base
de données

Sécurité du poste client



FortiClient
Solution de
sécurité du poste
de travail
FortiScan
Management des
vulnérabilités des
ressources

Services de mise à jour sécurité



FortiGuard
Service de mise à
jour des bases de
connaissances de
sécurité

Sécurité des Applications

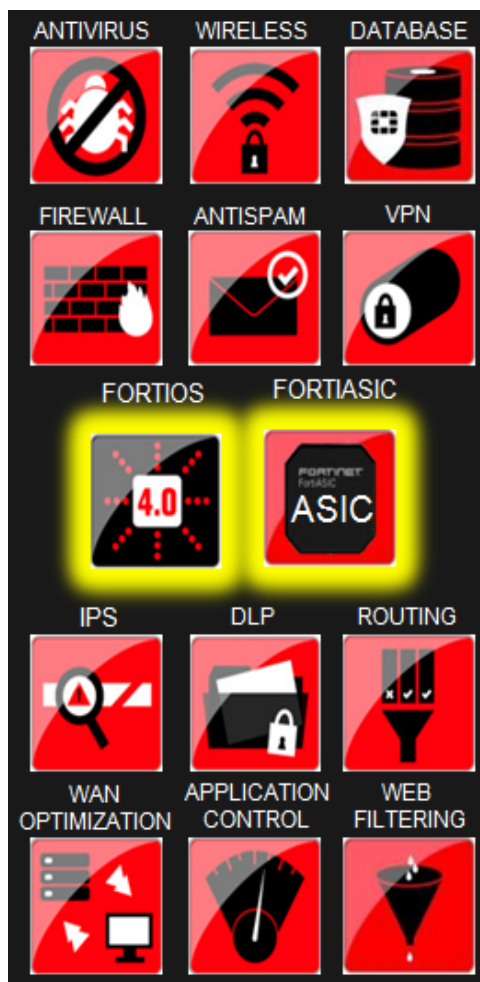


FortiMail
Sécurité de la
messagerie
FortiWeb
Sécurité des
applications XML
et web

5 FortiGate

FortiGate est une appliances de sécurité intégrant différentes fonctionnalités de sécurité aussi bien réseau qu'applicatif.

Les appliances sont extrêmement performantes du fait des processeurs propriétaires FortiASIC. FortiOS compile l'ensemble des fonctionnalités en un seul système.



Au niveau hardware, la gamme FortiGate est composée de plusieurs équipements pour répondre aux besoins de petites structures ou sites distants, que de réseaux d'entreprises, d'environnements opérateurs, fournisseurs d'accès et services Internet. Quelque soit l'équipement, l'administration, reporting, gestion de logs sont unifiés par les consoles FortiAnalyzer et FortiManager.



6 Les applications Fortinet

a. Firewall

La technologie de firewall Fortinet combine l'analyse «ASIC accelerated Stateful Inspection» et un arsenal d'applications de sécurité intégrées au moteur pour identifier et bloquer les menaces complexes. FortiGate® firewall est associé à des fonctionnalités clés de sécurité tels que VPN, antivirus, système de prévention des intrusions (IPS), filtrage Web, antispam et allocation de bande passante, lutte contre la perte d'information pour fournir une sécurité multi-niveaux aussi bien pour des appliances type SOHO/ROBO que des châssis multi-gigabit ou encore des plateformes pour datacenter. FortiManager™ et FortiAnalyzer™ sont les compléments clés des appliances fournissant une console de management centralisée pour des milliers de système FortiGate et la possibilité de générer de rapports ainsi que de réaliser des audits internes.

Les avantages de Fortinet Firewall

- FortiASIC™ permet d'assurer les fonctions de pare-feux et gestion du trafic avec des performances élevées en rapport avec les plateformes FortiGate.
- Intégration complète avec les autres technologies de sécurité Fortinet (ex : antivirus, filtrage web) pour une protection en profondeur.
- Sécurité virtuelle par domaines, zones réseaux, entités ou toutes autres divisions logiques ou physiques segmentées par les clients afin d'obtenir des politiques granulaires et une sécurité multi-niveaux.
- Trois modes opérationnels (transparent, NAT statique ou dynamique) pour s'adapter à une infrastructure existante et faciliter le déploiement en environnement hétérogène.
- Définition de nouvelles applications simplifiée permettant des politiques additionnelles granulaire et une protection plus précise.
- FortiClient, agent local, constitue une extension de la protection « firewall » sur les postes de travail, portables, Smartphones opérant en dehors du périmètre réseau.
- Les protocoles H.323, SIP et SCCP sont supports pour une protection des services VoIP.
- Support des protocoles dynamiques de routage (RIP, OSPF, BGP et PIM) en environnement réseau complexe.
- Haute disponibilité pour un service ininterrompu.
- Console de management et reporting centralisée facilitant l'exploitation tout en réduisant l'investissement et les coûts opérationnels.

b. IPS

La technologie Fortinet de prévention d'intrusion, disponible sur toutes les plateformes FortiGate® et FortiWifi™, embarquée dans les appliances ou châssis protège les applications critiques contre les attaques internes ou externes. Les mises à jours automatiques et en temps réel délivrées par le centre FortiGuard® Intrusion Prevention Service. FortiGate IPS associe une base de données paramétrable de plusieurs milliers de menaces connues afin de bloquer les attaques non reconnues par un firewall traditionnel et un système d'analyse comportemental reconnaissant les menaces pas encore répertoriées par le moteur de signatures. Cette combinaison de protection contre les menaces connues et inconnues, intégrée à la suite technologique Fortinet, permet de se prémunir contre les attaques critiques quelques soit la typologie : réseau filaire, sans fil, extranet ou interconnexions internes.

Les avantages de Fortinet IPS

- FortiASIC™ accélère les performances de détection d'intrusion aussi bien disponible sur les appliances SOHO que des châssis gigabit et plateformes de type « datacenter ».
- Combine moteur de signatures et analyse protocolaire pour une détection efficaces contre les menaces connues et inconnues, plus de 1 000 protocoles et applications sont supportés.
- Mises à jour automatiques par le centre FortiGuard Intrusion Prevention Service préservant ainsi les entreprises contre les dernières menaces.
- Souscription par équipement, nombre d'utilisateurs illimités, réduisant ainsi le coût total de possession.
- Console de management et reporting centralisée réduisant l'investissement et le coût d'exploitation de la solution de prévention d'intrusions.
- Logs et rapports détaillés facilitant les phases d'audit et les analyses légales.
- Haute disponibilité pour un service ininterrompu.
- Les modules « Bypass » disponible sur FortiGate assure un niveau de protection supplémentaire pour les segments de réseaux critiques.

c. VPN-IPSec et SSL

La technologie Fortinet IPSec et SSL VPN des plateformes FortiGate® est totalement intégré avec les autres fonctionnalités de sécurité tels que les pare-feux, antivirus, filtrage web et prévention d'intrusion fournissant un niveau de sécurité supérieur à des équipements VPN standard. La solution FortiGate VPN assure un niveau de performance nécessaire aux entreprises de toute taille, aussi bien des petites entreprises que des grandes organisations ou encore des fournisseurs de services Internet. FortiManager™ centralise la gestion de toutes les appliances jusqu'à plusieurs milliers de système FortiGate et facilite le déploiement parfois complexe à partir d'une seule console.

Les avantages de Fortinet VPN

- Les processeurs FortiASIC™ assure un niveau élevé de performances IPSec VPN aussi bien pour les équipements SOHO/ROBO que les châssis et plateformes.
- Support IPSec et SSL VPN pour un nombre illimité d'utilisateurs.
- Intégration avec les autres technologies de sécurité Fortinet pour une analyse multi-niveaux et multi-contenus assurant ainsi une protection efficace.
- Authentification étendue (RADIUS, LDAP, Base de données locale, SecureID, X-Auth) du client IPSec pour une totale interopérabilité.
- Support des protocoles de tunneling majeurs (IPSec, SSL, L2TP et PPTP) pour une implémentation flexible.
- Configuration possible en « hub-and-spoke » et « fully-meshed ».
- Capacité de prioriser les flux VPN à travers le module trafic-shaping pour optimiser la bande passante allouée.
- Certification FIPS 140-2 pour être en conformité avec les standards gouvernementaux américains.

d. Inspection SSL

La technologie SSL Inspection permet d'augmenter la sécurité et le contrôle de contenu en inspectant l'intérieur des flux chiffrés.

Les avantages de Fortinet Inspection SSL

- Inspecte les communications chiffrées.
- Augmente la protection pour la sécurité des serveurs et applicatifs Web.
- Augmente la visibilité du trafic réseau.
- Supports des protocoles HTTPS, POP3S, SMTPS, et IMAPS.
- Fonctionne sur le principe de « l'homme du milieu ».
- Choix de l'autorité de certification.

e. Wireless

La technologie Fortinet Wireless ajoute une protection essentielle au réseau local sans fils en intégrant des services tels que l'antivirus, prévention d'intrusion (IPS), filtrage web, antispam et gestion du trafic. La passerelle de sécurité FortiGate® fonctionne avec un point d'accès wifi de n'importe quel constructeur pour atténuer les faiblesses existantes et fournir une sécurité complète et performante pour n'importe quel WLAN. Les plateformes Fortifiai™ se déploie à partir d'un point d'accès wireless et broadband en environnement SOHO/ROBO, télécommuter et point de ventes. Les deux solutions sont supportés par FortiGuard® Security Subscription Services fournissant continuellement des mises à jour automatiques antivirus/antimalware, prévention d'intrusion, web filtering et antispam.

Les avantages de Fortinet Wireless

- Intégration de moteurs de scan antivirus, IPS, filtrage web, antispam pour une défense en profondeur des liens wireless.
- Mises à jour automatiques des signatures par FortiGuard Security Subscription Services pour protéger le réseau contre les dernières attaques et vulnérabilités.
- Console de management et reporting centralisée réduisant l'investissement et les coûts d'exploitation nécessaire à la sécurité wireless.
- Intégration de Fortifiai appliances à partir d'un point d'accès wireless réduisant ainsi les coûts d'implémentation et d'administration.
- La carte PC pour wireless 3G broadband (Fortifiai-60B) accélère l'intégration pour des points de ventes.
- Les différents niveaux d'authentification utilisateurs ou groupes d'utilisateurs permettent un contrôle fin des accès wireless vers les ressources internes en évitant l'accès par des individus malveillants ou d'autres points d'accès.
- Agent de sécurité léger FortiClient Mobile™ ajoute un niveau de sécurité sans fils des postes mobiles Windows, poste de travail, Smartphones notamment basé sur Symbian.
- Support de multiples méthodes d'authentification des utilisateurs, support d'annuaires pour améliorer l'administration et la sécurité.
- Le port IP/MAC permet une authentification physique aux terminal d'accès ce qui prévient les tentatives d'accès frauduleuses.
- Support de l'encryption forte pour suppléer aux faiblesses WEP et ainsi assurer un niveau de sécurité wireless élevé.
- Les politiques de gestion du trafic permettent d'allouer de la bande passante aux connexions wireless.

f. Optimisation WAN

Cette technologie permet d'optimiser les flux des applications communiquant au travers d'un réseau étendu tout en assurant une sécurité contre les différentes formes de menaces. Augmente les performances du réseau en réduisant le nombre de données transitant entre les applications et les serveurs sur le WAN

Les avantages de Fortinet Optimisation WAN

- Augmente les performances réseau.
- Réduit le nombre de données qui transitent à travers le WAN.
- Réduit les coûts réseaux liés à la bande passante entre clients et serveurs.
- Augmente la productivité de l'utilisateur en améliorant les temps de réponses.
- Fonctionne également entre FortiClient et FortiGate.
- Support de FTP, MAPI, CIFS, HTTP, TCP générique avec ou sans couche SSL.

g. Antivirus

La technologie antivirale de Fortinet® combine la détection par signatures avancées et moteurs heuristiques afin de fournir une protection multi-niveaux en temps réel contre les nouveaux et nouvelles variantes de virus, spyware, et malware propagés par le web, les emails et le transfert de fichiers. FortiASIC™, intégré à FortiGate® et FortiFai™ accélère la vitesse de scan et la détection des virus/malware aussi bien pour les équipements d'entrée de gamme que les appliances et châssis évolués. FortiGuard®, équipe de recherche des menaces et réseau global, fournit aux acteurs des mises à jours constantes pour une protection efficace contre tout type de contenu malveillant.

Les avantages de Fortinet Antivirus

- La technologie ASIC assure un haut niveau de performance d'analyse antivirale aussi bien pour les petits réseaux que les infrastructures multi-gigabit.
- Les mises à jour automatiques fournies par le service FortiGuard Antivirus assure aux entreprises d'être protégées contre les dernières menaces.
- L'agent FortiClient étend la protection antivirale sur les postes de travail, portables, Smartphones situés en dehors du périmètre réseau.
- La console de management et reporting centralisée couplée aux fonctionnalités de définition de zone de sécurité et domaines virtuels, réduit l'investissement et le coût d'exploitation lié à la protection antivirale.
- Souscription par équipement pour un nombre d'utilisateurs illimités limitant ainsi le coût total de possession.
- Différents modes d'implémentation (transparent, NAT, routage) pour que les appliances Fortinet s'adaptent à une infrastructure existante.
- Inspection des contenus encapsulés dans les protocoles SMTP, POP3, IMAP, FTP, HTTP, IM et P2P et support des formats de compression de fichiers principaux afin de fournir une protection efficace contre les différents vecteurs de propagation des menaces.
- Inspection des contenus à travers des connexions VPN pour une défense en profondeur avec support de tous les protocoles communs de tunneling (PPTP, L2TP, IPSec, SSL) et vérification de l'intégrité des hosts.

h. Antispam

La technologie Fortinet® antispam offre des fonctionnalités de détection, tag, mise en quarantaine et de blocage des spam et de leurs attachements malicieux. Les plateformes FortiGate® et Fortifai™ ainsi que l'agent FortiClient™ intègre les fonctionnalités d'antispam pour une protection multi-niveaux, supporté par le service FortiGuard™ Antispam. Les appliances FortiMail™ enrichissent l'offre via des fonctionnalités complémentaires pour se prémunir de la volumétrie du spam en croissance exponentielle ainsi que des Attaques de plus en plus sophistiquées. FortiMail permet également de disposer de fonction d'analyse de contenu, d'archivage, web mail en conformité avec les contraintes légales.

Les avantages de Fortinet Antispam

- Solution évolutive aussi bien pour les petites structures que les grandes entreprises et fournisseurs d'accès Internet.
- Les appliances FortiMail étendent les fonctionnalités pour une sécurité renforcée, incluant le scan des flux entrants et sortants, blacklist/whitelist, filtres antispam additionnel.
- Trois modes de déploiement de FortiMail pour un maximum de polyvalence, incluant l'application de serveurs de messagerie pour les structures de type SMB/SOHO.
- Politique de filtrage basée sur l'adresse IP, analyse de l'entête, analyse des images, contrôle de réputation via le service centralisé FortiGuard ainsi que d'autres méthodes de détection du spam pour fournir le plus haut niveau d'efficacité, par ailleurs certifié par le ICSA Labs.
- L'agent FortiClient étend la protection antispam au niveau des postes nomades, Smartphones utilisés en dehors du périmètre réseau.
- Console de management et reporting centralisée, fonctionnalité de zone sécurisée et domaines virtuels, réduisent l'investissement et les coûts d'exploitation nécessaire à une protection antispam.
- Capacité de stockage pour les appliances FortiMail, l'outil de log et reporting FortiAnalyzer facilité la mise en conformité légale concernant l'archivage d'emails.
- Modèle commercial basé sur les équipements, pour un nombre illimité d'utilisateurs, ce qui simplifie la protection des nouveaux utilisateurs sans surcoût additionnel et par conséquent réduit le coût total de possession.

i. Web filtering

La technologie Fortinet Web filtering, intégrée dans toutes les appliances FortiGate®, FortiFai™ et les agents pour postes de travail FortiClient PC™ bloquent les accès vers les sites web nocifs, inappropriés et dangereux contenant, par exemple, des attaques de type phishing/pharming, malware/spyware ou des contenus répréhensibles exposant l'entreprise à des poursuites judiciaires. Composé de bases de données reconnues et constamment mises à jour par FortiGuard® Web Filtering Service. Fortinet Web Filtering aide les organisations dans leur démarche de conformité légale et renforce l'utilisation appropriée d'Internet.

Les avantages de Fortinet Web filtering

- Utilisation de bases de données professionnelles de plus de deux milliards d'Url référencées offrant ainsi une protection contre les sites malicieux et à contenu non approprié.
- Classement en 77 catégories permettant une politique granulaire par utilisateur ou groupes d'utilisateurs et d'appliquer des règles d'accès à Internet afin de ne pas appliquer de restrictions abusives ayant un impact sur la productivité.
- Prix par équipement, nombre d'utilisateurs illimités soit une réduction du coût total de possession.
- Mises à jour automatiques de la base d'URL par FortiGuard Web Filtering Service afin que les organisations soient toujours protégées contre les derniers sites malicieux et inappropriés.
- Intégration complète avec Fortinet antivirus pour une protection totale contre les sites dangereux.
- Implémentation simple sans contrainte d'exploitation et d'administration complexe, idéale pour protéger les petites structures et les sites distants limités en ressources techniques locales.
- Certification CIPA et membre de la fondation Internet Watch Foundation (UK) pour l'aide à la protection des enfants, idéal pour les écoles et les bibliothèques.

j. Contrôle applicatif

La technologie Fortinet assure la reconnaissance et la mise en œuvre d'actions sur les communications en fonction de l'application à l'origine du flux au lieu de se baser sur un numéro de service ou un protocole. Cette solution renforce la politique de sécurité en appliquant une reconnaissance et un contrôle sur le protocole applicatif (indépendamment du port) utilisé pour la communication de plus de 1.000 applications courantes.

Les avantages de Fortinet Contrôle Applicatif

- Facilite l'inspection pour des applications qui utilisent des ports non standards, dynamiques ou "tunneliser" dans des protocoles couramment autorisés.
- Une politique plus flexible, plus fine et plus granulaire.
- Augmente la sécurité.
- Renforce la visibilité du trafic réseau.



k. Web Application Security

La solution Fortinet Web Application Security fournit une protection spécialisée, multi-niveaux pour les applications des grandes et moyennes entreprises, hébergeurs et fournisseurs Saas. FortiWeb fait parti de la famille des firewalls applicatifs destiné à protéger les applications Web et XML ainsi que les pages diffusées. Les plateformes FortiWeb fournissent une protection automatique et multi-niveaux contre les attaques sophistiqués tels que les injections SQL, Cross Site Scripting et pertes de données. Le module Web Vulnerability Assessment offre la possibilité d'effectuer des scans et par conséquent de se conformer aux exigences PCI DSS (section 6.6).

La solution FortiWeb réduit drastiquement le temps nécessaire pour protéger les données régulières, confidentielles ou propriétaires du site. FortiWeb accroît également la disponibilité des applications de manière intelligente en répartissant le trafic vers de multiples serveurs web. Cette répartition de charge améliore les performances, optimise l'utilisation des ressources et assure une meilleure stabilité des applications tout en réduisant le temps de réponse des serveurs.

Les avantages de Fortinet Web Application Security

- Répond aux critères de conformité PCI DSS (section 6.6) grâce à l'application de firewall applicatif et scan des vulnérabilités web.
- Protection en temps réel et multi-niveaux des applications web contre les attaques connues et inconnues tels que injection SQL et Cross Site Scripting.
- Mises à jour automatiques des signatures via le FortiGuard Security Service afin que les organisations soient toujours à la pointe en termes de protection contre les dernières menaces et vulnérabilités.
- Protection contre la perte d'information avancée assure la surveillance et la protection contre la fuite de données bancaires (numéro de cartes de crédit) et applicative par un contrôle fin du trafic sortant.
- Déploiement flexible et non intrusif permettant à FortiWeb d'être intégré à tout type d'environnement sans modification du réseau existant.
- Haute performance, la technologie FortiASIC reconnue et récompensée minimise le temps de latence, permet une accélération SSL ainsi que des fonctions avancées de répartition de charge.
- Base d'apprentissage évoluant automatiquement et dynamiquement pour une protection permanente des applications intégrant également la surveillance de l'activité des utilisateurs en temps réel.
- La surveillance "anti-mutilation" protégé les applications web contre les modifications non sollicités et restaure automatiquement la dernière version sauvegardée.

l. DLP

La technologie Fortinet DLP permet d'identifier et de se prémunir contre la fuite d'informations sensibles vers l'extérieur du réseau de l'entreprise

- Les avantages de Fortinet DLP.
- Protège les données sensibles de l'entreprise en repérant et bloquant leurs envois par le réseau.
- Peut fonctionner conjointement avec le contrôle applicatif y compris sur un flux SSL.
- Action configurable, blocage ou non, mise en quarantaine de la machine source.
- Permet un audit des fichiers entrants et sortants.
- Permet de se mettre en conformité avec certaines législations.

m. Database Security

Fortinet sécurité base de données et conformité offre de manière centralisée, renforcement de bases de données, politique de conformité rapide et efficace, gestion des vulnérabilités, supervision et audit pour un renforcement de la sécurité des données dans l'entreprise. La découverte automatique trouve toutes les bases de données sur le réseau y compris à travers les subnet et les frontières Wan. Les activités de bases de données sont superviser et auditer 24 x 7. L'ensemble des événements, les opérations utilisateurs sont capturés pour détecter les activités incorrectes ou malicieuses. Les enregistrements d'audit de toutes les activités des bases données sont stockés indépendamment pour plus de sécurité. Des centaines de politiques préconfigurées assurent le respect des standards, des règles gouvernementales et des meilleures pratiques de sécurité. Un ensemble complet de rapport fournit des indications immédiates. Ces rapports comportent des indications importantes concernant la conformité aux normes telles que PIC-DSS, SOX, GLBA et HIPAA. Fortinet Database Security and Compliance est disponible sous forme d'appliances ou logiciel pour grand nombre d'operating system.

Les avantages de Fortinet Database Security

- Déploiement initial rapide et intuitif, rapports fournissant immédiatement le niveau de protection.
- Haute performance des scans, découverte rapide des bases de données sur le réseau et à travers les infrastructures Wan et subnet, y compris les ports irréguliers.
- Améliore la sécurité et la conformité aux normes PCI, SOX, GLBA et HIPAA ?
- Des centaines de politiques préconfigurées couvrant les systèmes d'exploitations connus, faiblesse de configuration, failles OS, risques opérationnels, privilège d'accès aux données avec des mises à jour automatiques pour le respect des meilleures pratiques.
- Les politiques fonctionnent simplement et vérifient si les bases de données sont conformes à la configuration standard d'entreprise, réalisent des testes pour les applications particulières ou réalisent des conduisent des tests de pénétration prolongés, vérifient les password...
- Les enregistrements d'audit de l'activité des bases de données sont stockés indépendamment pour fournir un niveau de sécurité supplémentaire et assurer l'intégrité des informations d'audit.
- Les rapports standards et personnalisés sont exportables suivant la charte graphique de l'entreprise répondant aux règles de conformité avec des graphiques de tendances et données isolées.
- La supervision des activités de bases de données capturent toutes les types d'informations des événements de l'administrateur, des activités des utilisateurs au type de commandes (plain SQL, procédure de restauration) ainsi que le type de connections (ex : standard, console, pooled).
- Interface web de management centralisé disponible pour des multiples bases de données DBA, Oracle, DB2, SQL Server, Sybase, MySql pour identifier et réagir face aux vulnérabilités.
- Déploiement flexible à travers les réseaux de l'entreprise afin d'appliquer les politiques d'entreprise, capacité de gérer plusieurs dizaine de milliers de traces par jours.
- Solution disponible sous forme d'appliances pour plus de 60 instances de bases de données ou sous forme logiciel pour une variété d'OS et protéger ainsi des milliers de bases de données (licence par instance).