FORTINET

Equipements FortiGate

Présentation Technique

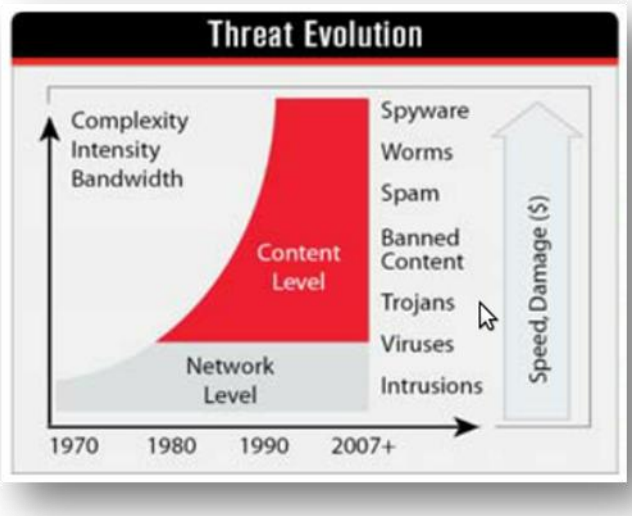
FROM :	Equipe SE Fortinet
TO :	
Copy :	No 1
Date :	Mars 2011
Reference :	Présentation Technique
Version :	1.1 Mise a jour en version 4.0

Table des matières

Analyse des menaces

C'est désormais un fait établi, la majorité des attaques pénétrant dans nos réseaux est embusquée dans les contenus véhiculés innocemment par les applications courantes du quotidien, qu'elles soient d'usage personnel ou professionnel. Cette tendance est d'autant plus vraie que la variété des moyens de communications ne cesse de se croître tout comme leur utilisation.

Les attaques d'aujourd'hui se caractérisent toutes par un objectif commun, du simple virus, ver, cheval de Troie, à la tentative d'intrusion en passant par leur usage cumulé pour une efficacité renforcée : infection d'un maximum d'équipements en un minimum de temps et installation d'un logiciel zombie permettant de prendre le contrôle de l'équipement et le faire participer avec des milliers d'autres équipements infectés à une attaque ciblée pour, par exemple, réaliser un déni de service.



Il y a 10 ans, les attaques étaient conçues par de jeunes hackers inconscients, par jeu ou challenge, pour la gloire ou la quête de reconnaissance de leur talent. Puis le milieu s'est orienté vers la captation financière et s'est considérablement organisé et criminalisé. L'avènement des botnets constitue aujourd'hui la pierre angulaire d'attaques à grande échelle permettant d'entrer dans l'ère de la cyber-guerre.

En termes de volumétrie, la courbe est exponentielle. Nous sommes passés de 50000 virus identifiés en l'an 2000, à plus de 200 millions en 2010. L'activité est tellement profitable que la production d'attaques s'est industrialisée. De véritables équipes de professionnels organisés comme dans une entreprise œuvrent à la conception d'attaques toujours plus sophistiquées. Il est aujourd'hui possible d'acheter des kits de botnets prêt à l'emploi pour un montant variant de 800 à 2000 dollars.

Il est difficile d'évaluer le poids financier de la cybercriminalité. Plusieurs critères peuvent être pris en considération comme les revenus générés directement par les attaques, les dommages subis par les entreprises, liés, par exemple, à la perte de productivité ou les coûts de mise à jour des équipements infectés. Il existe même un marché lucratif de vente de faux anti-virus.

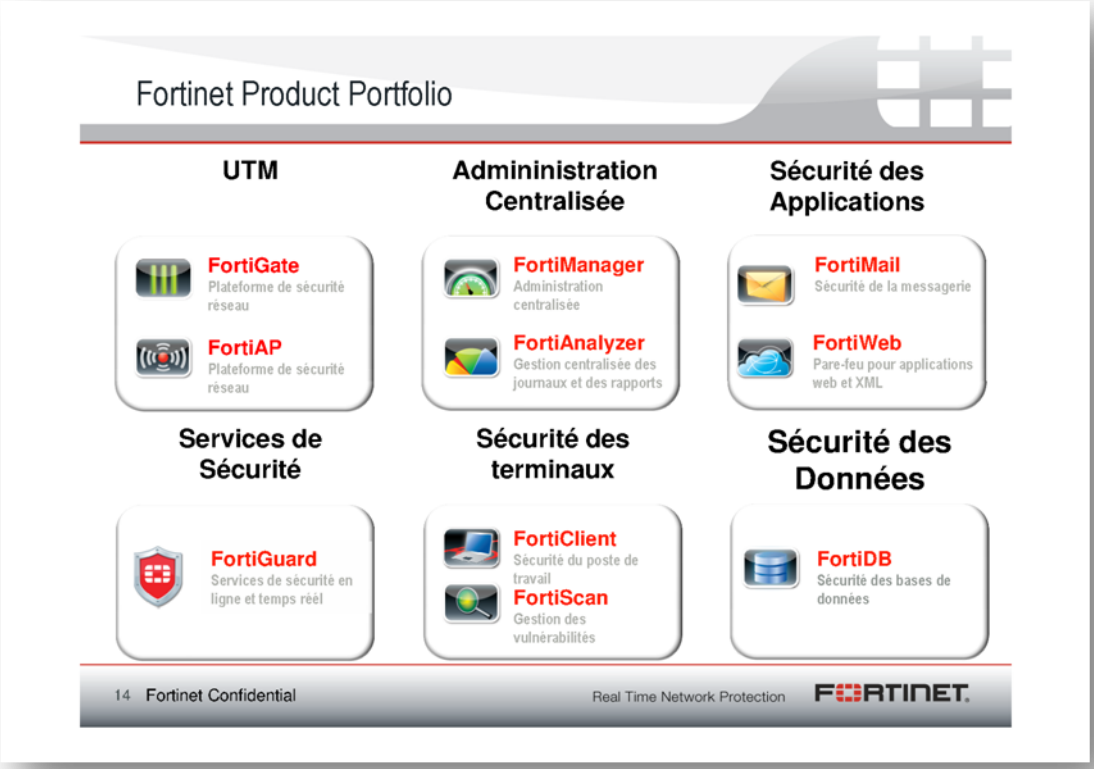
Le tout IP promis par l'arrivée prochaine d'IPv6 (tout équipement du quotidien pourra se voir attribuer une adresse IP : IP TV, domotique, automobiles, etc.) et le succès des terminaux dit intelligents (smartphone et tablettes communicantes qui, par nature, intègrent un système de

paiement automatisé via une taxation opérateur) constituent une telle manne financière que nous pouvons raisonnablement penser que la cybercriminalité n'est qu'à l'aube de son existence.

Positionnement de Fortinet

Le métier de Fortinet est de fournir des solutions de sécurité protégeant l'entreprise et ses utilisateurs des risques liés à l'exploitation de failles informatiques sur leur réseau, quelle que soit leur origine.

Fortinet est une société hautement technologique qui conçoit ses propres solutions de sécurité, principalement sous la forme d'*appliances* matériel mais également de logiciels. La gamme de produits proposée par Fortinet permet de mettre en œuvre une sécurité de bout en bout (poste de travail, serveurs, cœur de réseau, périmètre, nomades, sites distants).



Le contrôle multicouche des données transitant sur le système d'information est réalisé par la gamme des *appliances* FortiGate et FortiAP déployés en périphérie ou en cœur de réseau.

Le contrôle de conformité et la sécurité des postes de travail sont assurés conjointement par le logiciel FortiClient et l'*appliance* FortiScan qui effectue l'analyse des vulnérabilités du parc informatique.

Les applications web sont protégées par les *appliances* FortiWeb.

Leurs bases de données sont inspectées et analysées par FortiDB.

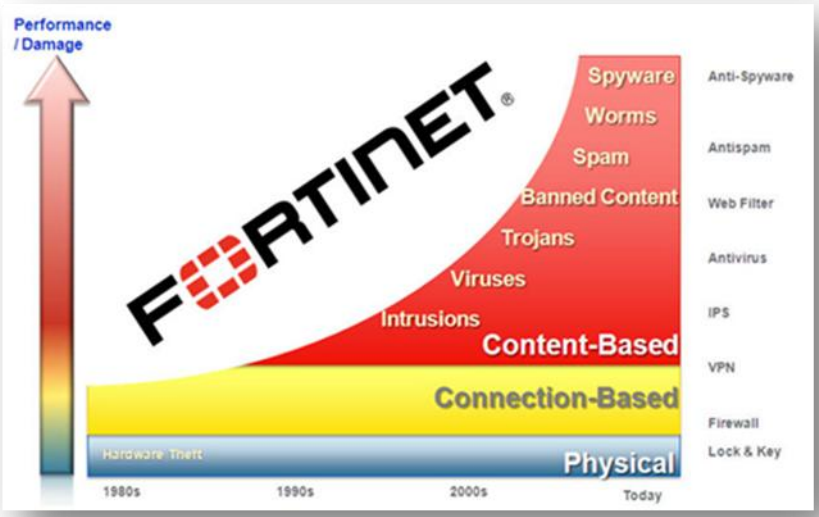
La messagerie est débarrassée des virus et des spams grâce aux *appliances* FortiMail qui mettent également en œuvre une politique de messagerie entrante et sortante.

Toutes ces *appliances* peuvent être administrées depuis une interface unique offerte par FortiManager. Enfin la centralisation des événements et la production de rapports et tableaux de bords sont obtenus par FortiAnalyzer.

La virulence des menaces et leur continuelle évolution nécessitent la prise en compte rapide des moyens de s'en protéger. C'est pourquoi les services FortiGuard, reposant sur un réseau distribué de mise à jour, permettent à l'ensemble des *appliances* de toujours disposer des dernières bases de signatures permettant de contrer ces menaces.

L'avantage Fortinet

Protection complète des contenus



Fortinet fournit une protection complète des contenus pour les réseaux d'aujourd'hui. Depuis les 10 dernières années les menaces ont évolué : ciblant autrefois les failles protocolaires et applicatives, elles sont désormais embarquées au sein même des contenus véhiculés par les réseaux. Les technologies de sécurité traditionnelles ne sont plus adaptées pour se protéger car elles ne savent plus faire la différence entre menace et contenu légitime.

Les menaces peuvent entrer dans votre réseau par le biais d'applications comme la messagerie électronique, votre navigateur Internet ou votre logiciel favori de réseau social.

Une protection efficace doit mettre en œuvre à la fois une identification des applications et des utilisateurs sur tous les contenus transportés.

Nos solutions hautement performantes de gestion des menaces unifiées fournissent la visibilité requise pour détecter des attaques cachées au sein du contenu légitime, même si elles proviennent de sources de confiance ou d'applications autorisées. Cette protection sans égale signifie que vous pouvez autoriser de nouvelles applications au sein de votre réseau et avoir la certitude de bloquer le contenu ou les comportements malveillants.

Chaque équipement FortiGate peut fonctionner en mode transparent ou en mode routé. Dans le premier cas, les paquets sont commutés d'une interface à une autre tandis que dans le second cas, ils sont routés. Il faut bien sûr qu'une politique de sécurité valide l'autorisation de transit de chaque paquet quelques soit le mode opérationnel.

Une fonction de virtualisation est également intégrée dans tous les équipements FortiGate. Elle ne se limite pas à décliner plusieurs instances de routages : chaque environnement virtuel est un FortiGate logique à part entière, disposant de toutes ses fonctions d'analyse multi-menaces (pare-feu, anti-virus, IPS, VPN IPSEC, SSL, contrôle applicatif, inspection SSL, etc.). Chaque FortiGate peut être virtualisé à hauteur de 10 instances. Une souscription dépendante du modèle permet d'étendre ce nombre jusqu'à 500 entités logiques au sein d'un seul équipement physique.

L'approche unique de Fortinet consiste à fournir le même niveau de sécurité du plus petit équipement au plus grand : en effet, tout *appliance* Fortinet propose les mêmes fonctionnalités.

Le modèle de vente de Fortinet ne repose pas sur une licence dépendante d'un nombre de fonctions, d'utilisateurs ou d'adresse IP. Chaque Fortinet dispose de toutes les fonctions sans surcoût. Le prix d'un équipement est dimensionné par son niveau de performance.

Leadership sur le marché

Fortinet est le leader du marché de la gestion unifiée des menaces (UTM), fournissant des solutions améliorant les performances, augmentant la protection et réduisant les coûts. Avec plus de 650 000 équipements vendus à ce jour, Fortinet sécurise les réseaux de plus de 100 000 clients dans le monde, incluant la majorité du Fortune Global 500.

Beaucoup de grandes entreprises et de fournisseurs de services parmi les plus expérimentés au monde font confiance à la technologie Fortinet pour sécuriser leurs réseaux et les données qu'ils transportent :

- 7 sociétés du classement américain « Top 10 Fortune »
- 8 sociétés du classement EMEA « Top 10 Fortune »
- 9 sociétés du classement APAC « Top 10 Fortune »
- Les 10 sociétés du classement "Top 10 Fortune telecommunications companies"
- 9 sociétés du classement "Top 10 Fortune banking companies "

Une protection certifiée

Fortinet est le seul constructeur de solutions de sécurité à avoir fait certifier l'ensemble de sa technologie.

Ces certifications, délivrées par des organismes reconnus et indépendants, démontrent notre capacité à intégrer de multiple briques de sécurité dans un équipement unique tout en conservant un haut niveau de performance et d'efficacité.

- 7 certifications ICSA Labs security
- Certification NSS UTM
- Certification ISO 9001
- 12 Virus Bulletin (VB) 100%
- Certification IPV6 et Critères Communs EAL 4+

Des performances incomparables

Les équipements conçus par Fortinet offrent des performances inégalées pour satisfaire les besoins croissant des réseaux. Notre technologie s'attèle à fournir la plus haute performance avec la plus faible latence du marché. Notre approche unique minimise le délai de traitement des paquets tout en inspectant efficacement son contenu, grâce notamment aux technologies d'accélération matérielle FortiASIC.

Très simplement, ces modules sont des processeurs spécialisés vers lesquels le trafic collecté est dirigé pour un traitement accéléré, permettant aux équipements FortiGate d'atteindre des niveaux de performance uniques (un chassis 5000 atteint les 500Gbps de throughput firewall).

Ils délivrent la puissance nécessaire pour détecter les contenus malicieux transitant à haut débit (de l'ordre du multi-gigabit). Leur rôle est d'assister, dans les traitements de type firewall mais aussi de type « applicatif » (Anti-Virus, IPS ou Contrôle Applicatif), le processeur central du système qui, de par leur volume, ne peut pas gérer efficacement l'ensemble des menaces véhiculées. L'intégration des FortiASIC dans nos *appliances* permet d'éviter de constituer un goulot d'étranglement dans le réseau protégé.

Trois catégories de FortiASIC peuvent être embarqués dans nos *appliances* :

- **FortiASIC Content Processor (CP)**

  Son rôle est d'assister le processeur central dans l'analyse AV/IPS des contenus inspectés. Il implémente un langage breveté par Fortinet appelé *Fortinet Content Recognition Language* qui décharge le processeur central des opérations de *pattern matching,* très consommatrices en ressources CPU.

  Il est également conçu pour générer, à grande vitesse, les clés de chiffrements négociées dans le cadre de VPN IPSEC ainsi que des fonctions de chiffrement et déchiffrement IPSEC/SSL.

- **FortiASIC Network Processor (NP)**

Situé au plus près des interfaces réseaux, l'objectif principal de cet ASIC est d'accélérer le traitement des paquets associés à une session VPN IPSEC ou à une session autorisée par la politique de sécurité.

Une fois pris en charge par l'ASIC, les paquets d'une session sont commutés d'une interface à une autre sans jamais solliciter les ressources du système. Les paquets restent localisés au niveau de l'ASIC, libérant ainsi des ressources système pouvant être allouées à d'autres tâches d'analyse.

L'ASIC NP est insensible à la taille des paquets et sa capacité lui confère une performance « à la vitesse de l'interface ».

- **FortiASIC Security Processor (SP)**

  Technologie reposant sur une architecture de processeurs multi-cœur (FGPA), le rôle de ce composant est décharger le système central du traitement des sessions autorisées par la politique de sécurité, des paquets transitant dans un tunnel IPSEC, des flux multicast et des tentatives d'intrusions (IPS).

Recherche Globale contre les menaces

Notre équipe FortiGuard composée de 125 chercheurs répartis sur le tout le globe assure une couverture horaire totale et une surveillance permanente des menaces en perpétuelle évolution. Elle alimente un réseau de mise à jour, le *Fortinet Distribution Network,* auquel sont abonnés tous les *appliances* de sécurité, afin de proposer automatiquement les mises à jours des différentes bases de signatures (AV, IPS) et fournir ainsi le meilleur niveau de protection dans les meilleurs délais.

La sécuritée intégrée Fortinet

FortiGate est un appliance offrant une combinaison intelligente de multiples fonctions de sécurité, dit *appliance UTM* (Unified Threat Management) ou *appliance* multi-services, mais également, ces derniers temps, *Firewall Next Generation.*

Avant de détailler l'ensemble des modules de sécurité embarqués dans un appliance FortiGate, nous allons mettre en avant les particularités clés qui en font leur originalité :

1. 100% Fortinet

L'appliance est développé à 100% par Fortinet. Cela signifie que le matériel, les composants d'accélération (ASIC ou FPGA), le système d'exploitation et les fonctions de sécurité sont entièrement conçues et développées par Fortinet.

Comme nous le verrons plus tard, il en résultera une capacité de fonctionnement unique en son genre (L2 ou L3, IPv4 ou IPv6, firewall physique ou virtuel) sans aucune dégradation fonctionnelle.

2. Pas d'OEM

Conséquence du point précédent, la plupart des fonctions de sécurité, et plus particulièrement celles en charge du contenu (antivirus, filtrage d'URL, IPS, contrôle applicatif, etc.) ont elles aussi été entièrement conçues et développées par Fortinet.

Un appliance FortiGate ne contient aucune technologie tierce (OEM) et n'est donc pas tributaire des aléas qui accompagnent ce type de partenariat :

- Risque de rupture technologique : le détenteur de la technologie n'est plus en mesure de proposer son module (racheté par un concurrent, cessation d'activité, etc.)
- Allongement des durées de traitement d'incidents (support) du fait des aller-retour entre le support constructeur et celui du partenaire OEM
- Paiement de royalties au partenaire OEM qui sont nécessairement répercutés dans le prix d'acquisition pour le client

3. Des certifications à jours

L'ambition de Fortinet est de répondre à la problématique de sécurité en proposant des modules sécurité simple, fonctionnellement complets – y compris en spécialisant l'équipement sur un module – et, surtout, validés par des instances tierces, reconnues sur le marché de la sécurité.

Nous mettons un point d'honneur à produire des certifications récentes1 qui sont autant de gages de crédibilité pour nos solutions.

4. Une intégration optimisée

Comment un acteur sécurité, concepteur de la totalité de ses fonctions, peut-il être meilleur qu'un acteur de niche, sur une thématique sécurité particulière ?

Nous avons une maîtrise totale de notre chaîne d'assemblage (matériel, système d'exploitation, et fonctions de sécurité). Dès lors, il est évident que le résultat final présente un niveau d'optimisation que les acteurs sécurité, dépendants de technologies tiers, ne peuvent reproduire.

Nous sommes par exemple en mesure de déporter des traitements "lourds" (firewalling, VPN, antivirus, IPS et contrôle applicatif) dans nos technologies d'accélération ASIC ou FPGA.

Nous ne sommes pas tributaires des contraintes produites par le module OEM d'un tiers lorsqu'il s'agit d'intégrer un nouveau module de sécurité dans nos appliances.

Notre culture historique "hardware" combinée à une recherche constante de nouvelle technologies d'assemblage, nous permet de réduire considérablement les coûts de fabrication et donc d'alléger la facture cliente. Ainsi, dernièrement notre technologie SoC (System on a Chip) nous a permi d'intégrer le 1Gbps accéléré par ASIC sur un appliance FGT-60C adressant le marché des petites et moyennes entreprises. Ces optimisations "hardware" nous permettent également de proposer des appliances très haut débits (FGT-3950B à 120Gbps, Chassis 5000 à 500Gbps) affichant des ratios prix/performance les plus intéressants du marché sécurité.

Ainsi, au fil des années, les nouveaux modules intégrés gagnent en maturité et en fonctionnalités, permettant d'adresser des problématiques de sécurité sur lesquelles un équipement firewall n'était auparavant et habituellement pas positionnable (passerelle antivirus, contrôle d'URLs avec authentification + gestion des temps de navigation, firewall next generation, etc.).

5. Une réactivité inégalée

Cette maîtrise totale de notre technologie a pour autre conséquence très importante de pouvoir offrir une capacité de réactivité très importante pour nos clients. Qu'il s'agisse de traiter un incident avec fourniture d'un correctif, ou bien de livrer une nouvelle fonctionnalité nécessaire à

http://www.fortinet.com/aboutus/fortinet_advantages/certifications.html

un projet d'envergure, nos ingénieurs R&D, pleinement maîtres de leur environnement, savent réagir rapidement et efficacement.

FortiOS 4.0 – Redéfinir la sécurité réseau des entreprises

Avec des débits de plus en plus élevés, les réseaux d'aujourd'hui transportent toujours plus d'informations et de contenus structurés où se mêlent parfois des attaques malicieuses. Le volume et la sophistication de ces attaques ont malheureusement une croissance à un rythme similaire.

Il est désormais nécessaire de mettre en place des moyens de détection plus rapides, plus fiables et capables de bloquer les attaques avant qu'elles ne créent des dommages préjudiciables au sein de l'entreprise.

FortiOS est un système d'exploitation renforcé conçut exclusivement pour servir de fondations logicielles communes à toutes les plates-formes de sécurité intégrées FortiGate.

Offrant, dans un unique appliance, la suite de sécurité et de services réseaux, opérationnel pour IPv6, la plus complète, il tire profit de l'accélération matérielle offerte par les processeurs FortiASIC.

Le service de veille & de distribution FortiGuard vient le compléter en fournissant les mises-à-jour des signatures des outils de protection intégrés à FortiOS. Les entreprises sont ainsi efficacement protégées contre les dernières attaques, aussi sophistiquées soient-elles.

Nous présentons ci-après les points forts du système d'exploitation FortiOS 4.0.

Une sécurité complète

La stratégie de Fortinet est donc de développer ses propres modules de sécurité puis de les intégrer à FortiOS afin d'offrir un niveau d'efficacité en terme de visibilité, sécurité et de performance que ne peuvent pas atteindre les solutions de sécurités dédiées, traditionnellement simplement empilées dans l'environnement à protéger.

Cette combinaison intelligente de modules de sécurité dans FortiOS offre naturellement une meilleur visibilité et un meilleur contrôle sur le traitement des dernières attaques, avant que ces dernières ne puissent nuire à l'entreprise.

Une visibilité et un contrôle unique

Les modules de sécurité de dernière génération, tels que le profilage actif, l'inspection anti-virus en mode flow ou bien le contrôleur Wireless, permet de garantir une protection qui va du poste de travail jusqu'au cœur du réseau, et des sites distants d'agences jusqu'aux sites principaux ou datacenters.

FortiOS offre une visibilité accrue sur le trafic et permet un contrôle plus consistant et granulaire des utilisateurs, des applications et des données sensibles transportées.

Les modules sécurités de FortiOS 4.0

Cette section présente les modules de sécurité intégrés dans FortiOS 4.0.

La plupart de ces modules sont activables à la demande, sans utilisation de licence spécifique. Certains modules, comme le module anti-virus ou le module IPS, sont simplement liés aux services de mises à jour FortiGuard et nécessitent donc la souscription à un abonnement.

Les modules de sécurité intégrés dans FortiOS 4.0 sont :

- un firewall d'entreprise (IPv4 et IPv6)
- un concentrateur VPN IPSEC et SSL
- Inspection du trafic SSL
- Anti-virus et Anti-spyware
- Antispam
- Système de prévention d'intrusions (IPS)
- Système de prévention de fuites d'informations (DLP)
- Mécanisme d'analyse en mode flow
- Filtrage web
- Contrôle applicatif
- Profilage actif
- Fonction de contrôle d accès réseau (NAC) pour le poste de travail
- Système de gestion des vulnérabilités
- Systèmes de gestion des logs et de génération de rapports
- Optimisation WAN
- Contrôleur Wireless
- Système de sécurisation de la VoIP

- Administration centrale
- Virtualisation (technologie Virtual Domain ou VDOM)
- Système de haute-disponibilité
- Services de routage L2/L3
- Système de mise à jour FortiGuard

FortiOS 4.0 – Une protection complète des contenus et des réseaux

Fortinet continue d'innover en matière de standard concernant les modules de sécurité et réseau, intégrés au système d'exploitation FortiOS, spécifiquement conçu pour la sécurité.

Engagé dans un cycle où s'ajoutent constamment de nouveaux modules de sécurité, et où les performances de ceux existant sont améliorés en permanence, le système d'exploitation FortiOS démontre qu'il est la référence en matière de firewall sécurité multi-services.

Modules avancés de sécurité

Le système d'exploitation FortiOS 4.0 comprend plusieurs modules réseau ou de sécurité avancée. Certains d'entre eux sont présentés ci-dessous

Le contrôle applicatif

Le contrôle applicatif est un module permettant de définir et d'appliquer des politiques de sécurité concernant plus d'un millier d'applications véhiculées par les réseaux ou s'exécutant sur les postes de travail.

Les nouvelles applications web telles que Facebook, Skype, Twitter ou Salesforce.com peuvent ainsi être détectées et contrôlées de manière très granulaire, sans aucune contrainte sur les ports ou protocoles (TCP ou UDP) utilisés.

La classification et le contrôle des applications sont devenus des opérations essentielles pour contrebalancer l'explosion des technologies essentiellement orientées Internet et bombardant les réseaux aujourd'hui.

Le profilage actif

Le profilage actif permet de détecter et de réduire les attaques par la construction d'une courbe de référence d'utilisation. Tout comportement réseau sortant du cadre de ce référentiel est alors considéré comme une menace potentielle.

Le volume de trafic, le nombre de connexions, les informations géographiques sont autant de paramètres utilisés la constitution du référentiel

En cas de non respect du référentiel, des mécanismes de réponses automatisés peuvent être déclenchés, tels que la mise en quarantaine ou le blocage du *malware* ou de l'utilisateur indésirable.

Anti-virus et anti-spyware

En plus des trois bases de signatures (standard, étendue et extrême) utilisables par le moteur anti-virus en mode proxy, FortiOS propose un moteur anti-virus haute-perfmance en mode *flow*. L'utilisation du mode *flow* permet de prendre en charge des objets sans contrainte de taille, tout en maintenant les plus hauts niveaux de vitesse d'analyse.

Le mode *flow* implémenté dans FortiOS analyse les objets présents dans des archives compressées de manière à déjouer les tentatives d'insertions de virus masqués.

L'utilisation du moteur anti-virus en mode proxy ou mode flow est très flexible (par VDOM ou même par règle !). L'administrateur peut ainsi faire correspondre le niveau de sécurité et de performance d'analyse anti-virus, avec le niveau d'exigences souhaitées par son entreprise.

Système de prévention de fuites d'informations (DLP)

Le système DLP de Fortinet identifie les informations sensibles et bloque leur transmission vers l'extérieur du périmètre de l'entreprise.

Un moteur sophistiqué d'analyse par *pattern-matching* scrute le trafic généré par les applications connues pour le transport d'objets (messagerie, web, messagerie instantanée chiffrée, etc.) et conserve une trace de leurs utilisations pour la mise en conformité avec les nouvelles réglementations d'entreprise.

L'administrateur peut s'appuyer sur un éventail large d'actions de contre-mesure : log, blocage, archivage, bannissement ou mise en quarantaine.

Le système DLP fonctionne en mode proxy ou *flow*.

Filtrage web

La problématique est désormais bien connue : la consultation de sites web inappropriés, et l'utilisation croissante des applications web sont des comportements générateur de problème de productivité ou de congestion réseau, et de risque d'infection ou de perte de données.

Le filtrage web supprime ces problématiques en contrôlant l'accès par les utilisateurs, aux applications web tels que les messageries instantanées, les systèmes de partage peer-to-peer, ou les sites de streaming de médias. Dans le même temps, le filtrage web bloque les sites « hameçon » (phishing), les systèmes de botnets pilotés par commandes web, ainsi que les sites de téléchargement rapide.

Le filtrage web fonctionne en mode proxy ou en mode *flow*.

Contrôleur Wireless

Tous les appliances FortiGate et FortiWifi disposent du module contrôleur wireless. Ils peuvent donc administrer de manière complètement centralisée les réseaux wireless ainsi que les points d'accès FortiAP qui les portent.

Les flux collectés par les points d'accès FortiAP sont aspirés par le contrôleur wireless, le FortiGate. Ce dernier peut ainsi mettre en œuvre sa batterie de modules sécurité et ainsi bloquer les flux non autorisés tout en activant des mécanismes d'inspection avancée pour les autres flux.

L'administrateur peut contrôler simplement ses accès réseaux wireless, mettre à jour très rapidement les politiques de sécurités wireless et identifier les points d'accès non autorisés – le tout depuis une console unique connectée sur l'appliance FortiGate ou FortiWifi.

Optimisation WAN

Le mécanisme d'optimisation WAN accélère les applications, dont les communications s'opèrent à travers des liens WAN, tout en cohabitant avec les autres modules de sécurité intégrés dans FortiOS qui ainsi maintiennent un contrôle sécurité avancé sur les applications accélérées.

Le système d'exploitation FortiOS 4.0 élimine le trafic inutile et anormal tout en optimisant le trafic légitime par la réduction du volume d'informations transmis

par les applications.

Le bénéfice est double : amélioration des performances des applications et des services réseaux tout en réduisant les besoins (et donc les dépenses) en bande passante supplémentaire.

Ces techniques intègrent l'optimisation protocolaire, le cache d'octets et d'objets, les foncions d'offload SSL et les tunnels sécurisés. L'optimisation protocolaire améliore l'efficacité et diminue la sensibilité à la latence des flux qui utilisent CIFS, FTP, HTTP ou MAPI aussi bien que le trafic générique TCP. Les fonctions de cache permettent de réduire au minimum le volume de données qui transite entre les sites. Quant aux fonctions d'offload SSL, elles permettent de déporter le chiffrement sur l'équipement qui bénéficie d'accélération matérielle. Les tunnels sécurisés permettent d'assurer la confidentialité des informations en transit sans pour autant solliciter de ressource au niveau des applications et des postes.

Un firewall d'entreprise (IPv4 et IPv6)

La technologie firewall de Fortinet combine un mécanisme de stateful inspection (compatible avec les technologies d'accélération FortiASIC) avec un arsenal intégré de modules de sécurité avancés, avec pour bénéfice une efficacité redoutable dans l'identification rapide et le blocage des attaques évoluées.

Le firewall Fortinet s'intègre naturellement avec d'autres modules clés, tels que le concentrateur VPN, le moteur anti-virus, le système de prévention d'intrusions (IPS), le mécanisme de filtrage web, le moteur antispam, le système de QoS, etc. pour délivrer une sécurité multi-couche adressant aussi bien les besoins des petites entreprises que les besoins des sites centraux ou des datacenters équipés de cœurs de réseaux multi-gigabit.

Système de prévention des intrusions (IPS)

Le système de prévention des intrusions (IPS) apporte une protection contre les menaces réseaux existantes et émergentes.

Le système IPS de Fortinet s'appuie sur deux mécanismes : le premier est orienté détection par signatures, le second est orienté détection par anomalies.

Le mécanisme de détection par anomalie déclenche des alertes lorsque le comportement du trafic analysé peut correspondre au comportement d'une nouvelle attaque. Ce comportement anormal est ensuite analysé par nos centres de recherches Fortinet afin d'identifier clairement l'attaque et générer une

nouvelle signature qui sera immédiatement injectée dans notre système FortiGuard pour une publication rapide à tous les appliances FortiGate abonnés à ce système *cloud* de mise à jour de signatures.

Concentrateur VPN IPSEC et SSL

La technologie VPN de Fortinet apporte des moyens de sécurisation des communications, effectuées entre de multiples réseaux et postes de travail, par l'utilisation des protocoles IPSEC et SSL.

La technologie d'accélération matérielle FortiASIC permet de prendre en charge les opérations complexes afférentes à ces deux protocoles, tant dans les phases de négociations que dans les phases d'échanges de données ou de communications.

En sortie de tunnel IPSEC ou SSL, les modules sécurité intégrés au système d'exploitation FortiOS 4.0 sont pleinement utilisables pour ajouter une touche optionnelle de traitement sécurité avancées du contenu.

Antispam

La technologie Antispam de Fortinet offre une abondance de mécanismes pour détecter, marquer, mettre en quarantaine et bloquer les spams et pièces jointes suspectes générés par les environnement spambots ou les postes compromis.

Les solutions FortiGate, FortiWifi et FortiClient intègrent à part entière la technologie antispam dans la stratégie Fortinet de sécurité multi-couche concrétisée par le regroupement intelligent des différents modules de sécurité évoqués jusqu'à présent.

La technologie antispam intégrée dans les solutions FortiGate, FortiWifi et FortiClient est épaulée par le service antispam FortiGuard.

Mise en application des modules avancés de sécurité

La règle firewall sera le dénominateur commun.

Pour une plus grande souplesse dans l'utilisation de multiples modules de sécurité, toutes les mesures sécuritaires seront activées par règle firewall.

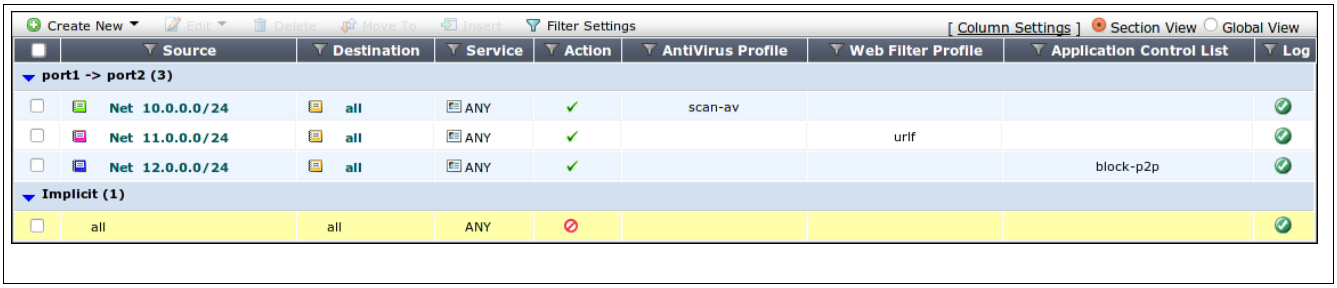
La figure suivante présente une partie des propriétés d'une règle firewall.

- Jusqu'à l'intitulé « Action », nous avons les paramètres usuels d'une règles firewalls :
    - L'intitulé « Schedule » permet de prendre en compte une plage horaire récurrente ou fixe dans le temps.
    - L'intitulé « Services » permet de définir le ports correspondant à l'application que nous souhaitons contrôler.

- L'intitulé « Action » clôture la zone réservée au mécanisme firewall stateful et précise l'action à effectuer sur le trafic correspondant à cette règle. L'action peut-être « Accept », ou «Deny». Une troisième action existe, « IPSEC » et ouvre l'accès au module concentrateur VPN IPSEC.

- La zone « UTM » permet d'illustrer très simplement que l'activation des modules de sécurité s'effectue par règle :
  - Si elle est cochée, la directive « Enable AntiVirus » active le moteur antivirus
  - De même, la directive « Enable IPS » activera le système de prévention des intrusions
  - Et ainsi de suite pour toutes les autres directives (« Enable Web Filter », « Enable Email Filter», etc.).

Les modules de sécurité étant activés règle par règle, l'administrateur sécurité dispose d'une très grande souplesse et d'une granularité complète quant à leurs utilisations. L'exemple ci-dessous en est une excellente illustration :



- Dans cet exemple, les trois règles utilisées sont associées à un module sécurité différent
  - Le trafic provenant du réseau 10.0.0.0/24 sera pris en charge par le moteur antivirus. Ce dernier analysera le trafic conformément aux paramètres déclarés dans le profile « scan-av ».
  - Le trafic provenant du réseau 11.0.0.0/24, sera quant à lui pris en charge par le mécanisme de filtrage web pour appliquer une politique de filtrage d'URL défini dans le profile « urlf ».
  - Le trafic provenant du réseau 12.0.0.0/24 sera finalement pris en charge par le module de contrôle applicatif pour détecter et bloquer l'utilisation des applications peer-to-peer.

- La zone « Traffic shaping » intègre des fonctionnalités de gestion de trafic et de qualité de service permettant de lisser le trafic avec la granularité d'une règle de pare-feu, d'un groupe d'utilisateur ou encore d'une adresse IP. Les fonctionnalités disponibles sont :

- bande passante garantie, ce qui assure à l'utilisateur qu'en cas de congestion du réseau, une partie de la bande passante totale sera réservée au trafic associé à ce module de contrôle.
- Bande passante maximale, qui permet de limiter le flux associé à ce contrôle à une valeur maximale.
- Affectation d'un niveau de priorité parmi trois valeurs possibles (high, low ou medium). Le champ inspecté correspond au champ standard DSCP de la couche IP. Il est possible d'affecter une valeur fixe au champ (diffServ/ToS) et différente pour les flux entrants et sortants.
- Affectation d'un quota : il est possible d'assigner aux modules de contrôle des quotes-parts. Il est ainsi possible pour un flux donné de stipuler un volume maximal de données par unité de temps, par exemple 10 Mo par heure ou 1 Go par jour.

Les fonctions de traffic shaping mettent en œuvre des techniques de bufferisation et de lissage pour réguler le trafic selon un débit particulier. Les paquets qui dépassent un seuil sont mis en attente dans des buffers. Contrairement à une police stricte, le traffic shaping tente d'éviter que les paquets ne soient rejetés lorsque les débits sont trop importants. Il ajoute un temps de latence aux données en stockant les paquets dans des buffers avant leur envoi sur le réseau.

Flexibilité d'intégration

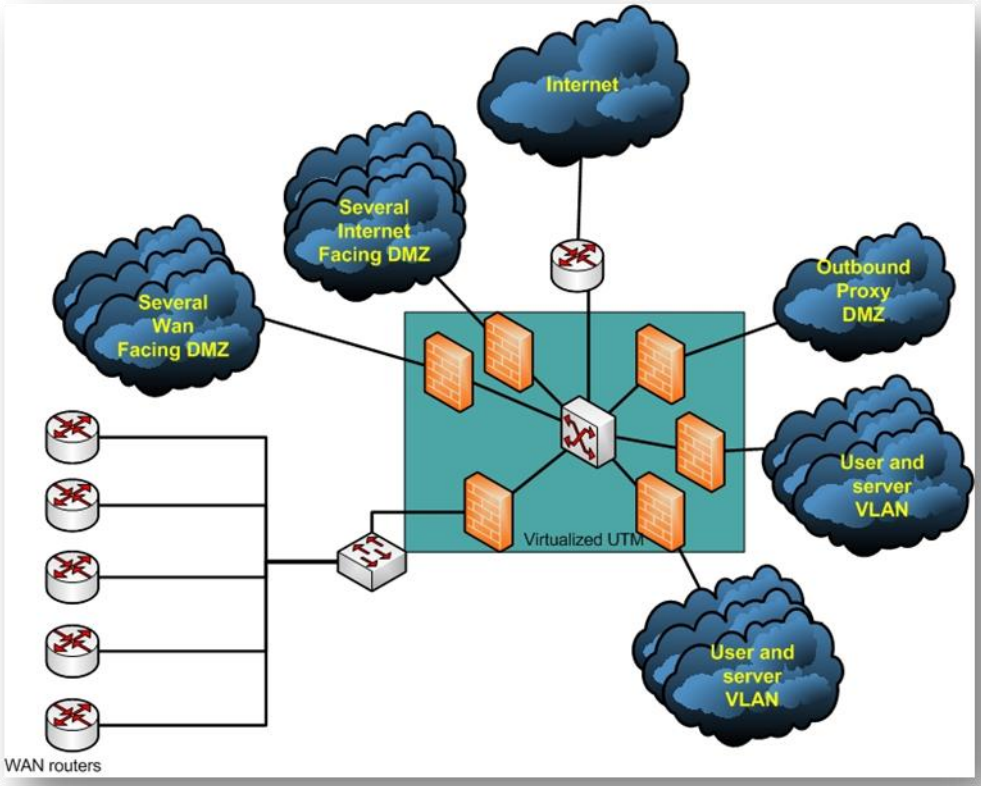
Virtualisation intégrée

Une des principales caractéristiques des FortiGates est de disposer d'un large éventail de fonctions leurs permettant de s'intégrer facilement dans les architectures en place. L'ensemble de ces fonctions pouvant intéragir ensemble cela donne une grande flexibilité d'intégration et d'utilisation.

Chaque FortiGate supporte en natif la notion de Virtual Domain ci-après nommé Vdom. Ceci correspond en fait a des instances virtuelles différentes et étanches pouvant être administer de façon indépendante par des administrateurs différents. A l'exception du FG30B tout FortiGate dispose de la possibilité d'utiliser de 1 à 10 Vdoms sans surcoût. A partir du modèle FG1240B il est possible d'étendre ce nombre d'instances virtuelles par licences. La limite maximum de nombres de Vdoms est de 25 sur un FG1240B et de 250 à partir du FG3016B.

Dans une instance virtuelle, l'ensemble des fonctions du FortiGate sont virtualisées. Vous disposez donc non pas de simples instances de pare-feux et table de routages différentes mais bien d'instances multi-fonctions de sécurité pouvant avoir chacune leurs propres paramétrages et spécificités. Chacune des instances du FortiGate peut fonctionner dans l'un des deux modes de fonctionnement du FortiGate (mode routage ou transparent) et se voit alors affecté des interfaces (réelles ou virtuelles) sur lesquelles elle travaillera. Il est donc ensuite possible, si nécessaire, de réaliser un maillage de ces instances virtuelles soit par des cables soit par un lien virtuel entre deux Vdoms routés portant le nom de Vdom link.

Il est ainsi possible de réaliser avec un seul FortiGate l'architecture suivante :



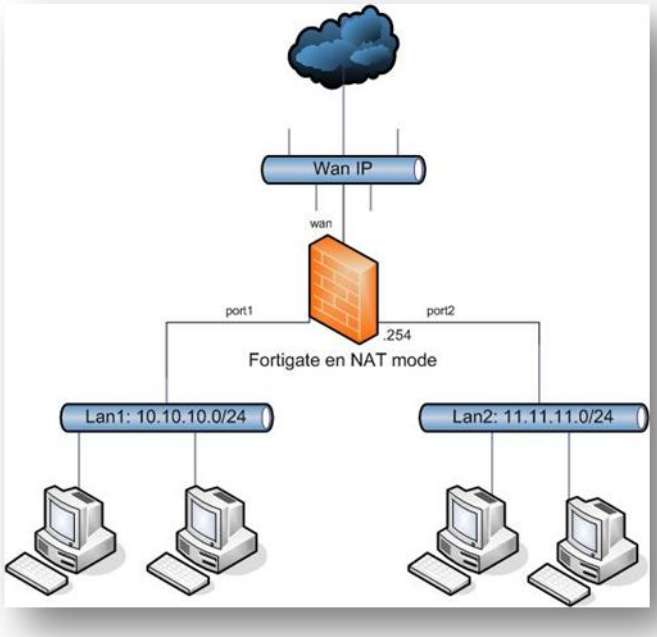
Il est possible à tout moment de passer du mode réel au mode virtuelle sans perdre sa configuration actuelle. Cette dernière est tout simplement convertit en la configuration de la première instance virtuelle, le Vdom root.

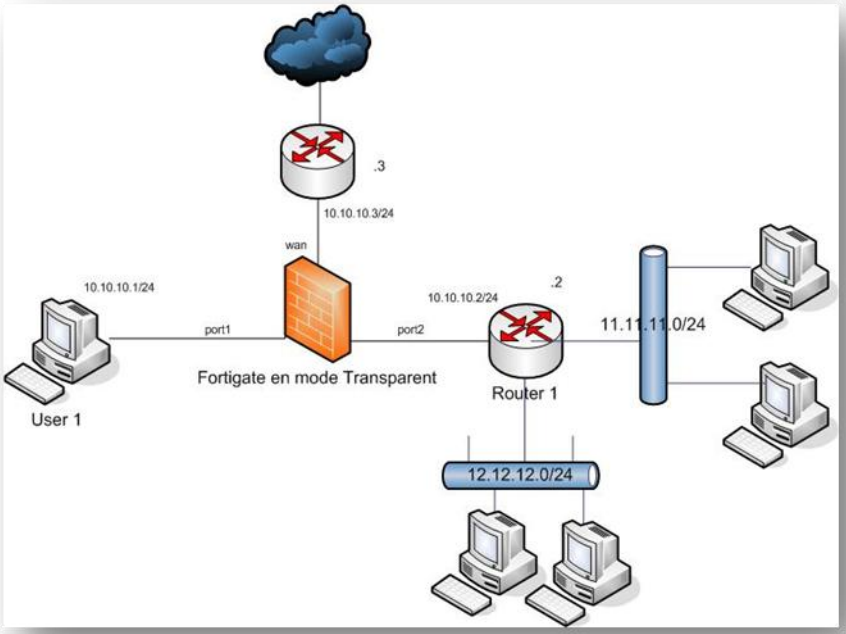
Contrairement à d'autres solutions de virtualisation il n'y a pas simulation de machines virtuelles sur chacune desquelles ont fait tourner un système d'exploitation, c'est directement le FortiOS qui prend en charge cette virtualisation. Ceci permet de pouvoir préciser pour chaque instance des valeurs garanties et/ou maximums sur une liste de ressources utilisées par le FortiGate. Ainsi on peut garantir à une instance quelle pourra géré X sessions simultanées alors qu'une autre instance, au contraire, pourrait volontairement être brider.

Mode routage ou mode transparent

Chacune des instances du FortiGate peut fonctionner au choix en mode routage ou transparent. En mode routage leur FortiGate dispose d'une ou plusieurs adresses sur chacune de ses interfaces et se comporte alors au niveau réseau comme un routeur niveau 3. Dans ce mode il y a donc consultation d'une table de routage pour décider des interfaces de sorties. Ces contraintes de routages peuvent être soit statique, soit de type PBR routage sur une politique définie ne tenant pas uniquement compte de l'adresse destination, soit par routage dynamique (RIP, OSPF, BGP, IS-IS), soit dans le cadre du routage de paquets multicast (PIM). C'est également dans ce mode que la translation d'adresse est le plus couramment utilisée d'où son nom parfois de mode NAT.

En mode transparent, l'instance du FortiGate est vue par le réseau comme un pont ethernet. Toutefois, le FortiGate fait tout de même de l'analyse sur les couches 3 à 7 du modèle OSI. Ce mode à l'avantage de ne pas nécessité de modification du plan d'adressage pour positionner le FortiGate en mode coupure. Il n'a alors plus d'adresse IP à l'exception de celle utilisée pour le management et qui est généralement uniquement portée par une interface dédiée à cette tâche. A l'exception du routage, toutes les fonctions du FortiGate sont disponibles dans ce mode toutefois certaines sont plus limitées qu'en mode routé.





Virtualisation au niveau des interfaces

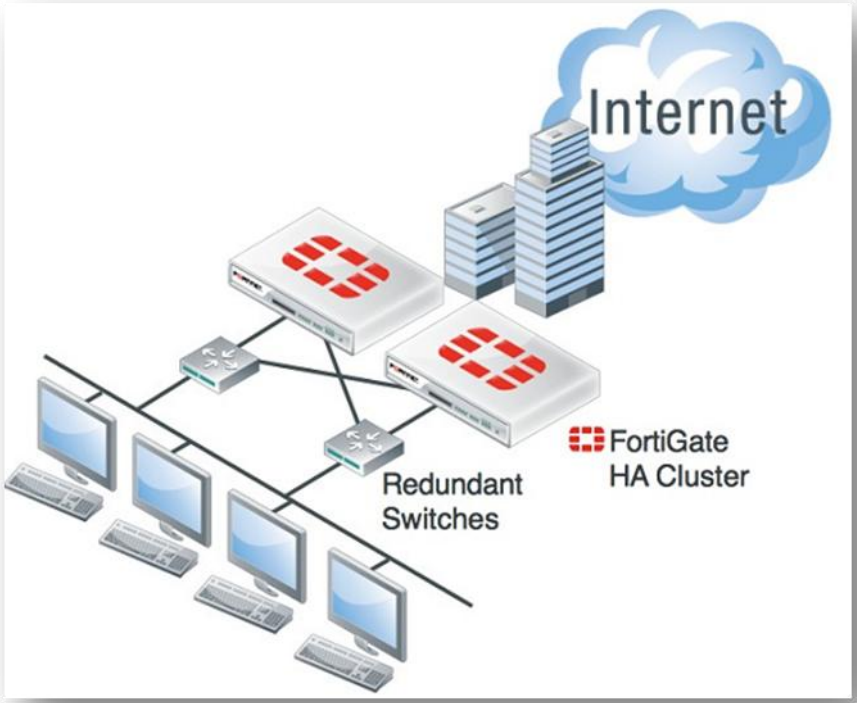
Sur un FortiGate, à l'exception du FG30B qui est particulier, on désigne par le terme « interface » différentes choses :

- une interface physique (cuivre, fibre, connecteur SFP ou XFP)
- un SSID pour les équipements avec point d'accès wifi
- une interface redondante (au moins deux interfaces physiques se suppléent l'une l'autre)(supporter à partir du modèle FG300)
- un aggrégat de ports physiques en 802.3ad (LACP))(supporter à partir du modèle FG300)
- une interface virtuelle (interface VPN SSL, interface VPN IPsec, interface Vlan, Vdom link, interface GRE, interface WebProxy)

Toutes ces formes d'interfaces ont leurs utilités et contribuent largement à la flexibilité d'intégration des FortiGates.

Haute disponibilité

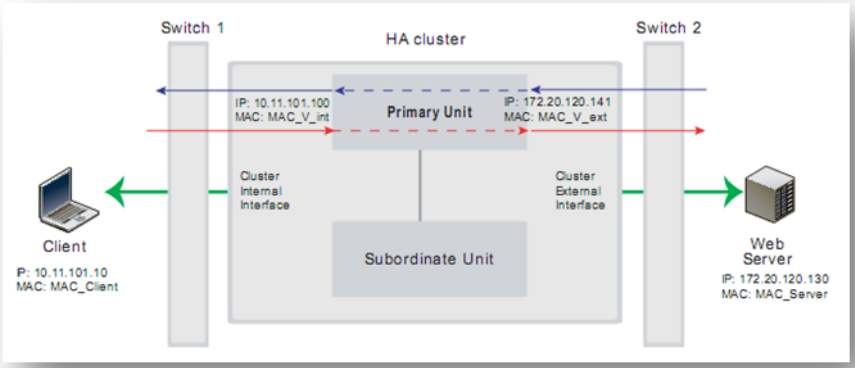
FortiOS intègre une fonction avancée de haute disponibilité permettant la mise en œuvre d'architectures de sécurité hautement redondantes.



La haute disponibilité de FortiOS repose sur le protocole propriétaire de niveau 2 FortiGate Clustering Protocol (FGCP) qui propose un mécanisme de surveillance des nœuds constituant le cluster ainsi que la synchronisation de leur configurations et de leur informations dynamiques (sessions, table de routage, etc.).

Un cluster peut se décliner en mode actif-passif (A-P) ou actif-actif (A-A). Dans tous les cas un processus strict définit un nœud jouant le rôle de maître. Les autres sont alors considérés comme des nœuds secondaires. Le maître prend en charge tout le trafic entrant sur le cluster. En mode A-P, les nœuds secondaires permettent de reprendre l'activité d'un nœud maître dysfonctionnant.

En mode A-A, le nœud maître redistribue le trafic sur ses membres secondaires en fonction d'un algorithme paramétrable.

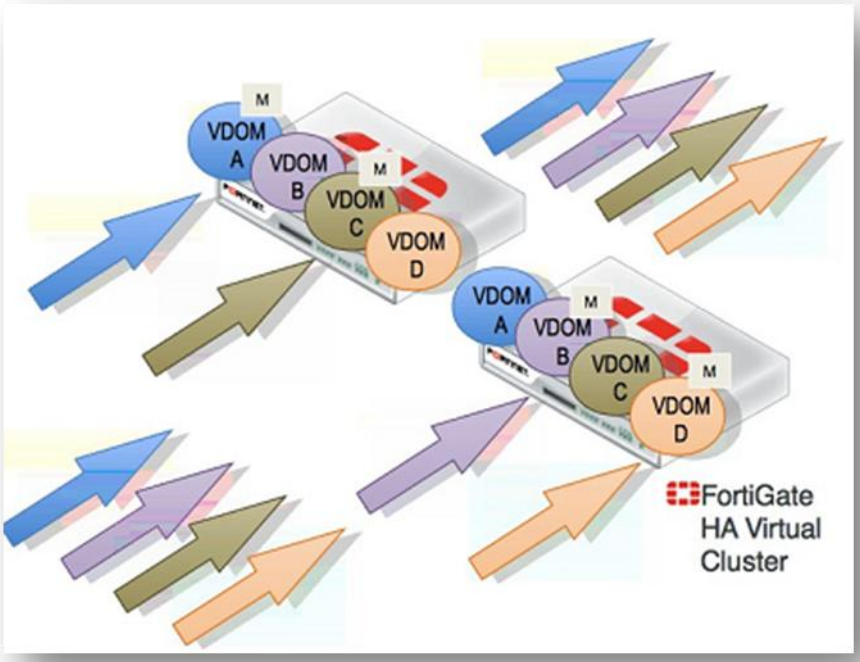


FGCP simplifie grandement l'administration d'un cluster de plusieurs nœuds. En effet, un cluster est considéré comme un unique équipement. Le nœud maître porte une adresse IP et MAC virtuelle différente pour chacune de ses interfaces. En cas de défaillance, le prochain nœud préempté reprend la gestion de ces adresses. Le trafic est alors automatiquement transmis vers ce nouveau maître au terme d'un délai de convergence pouvant être optimisé voire être inférieur à la seconde.

La haute disponibilité de FortiOS propose la fonction *uninterruptible upgrade*. Elle consiste à déclencher une mise à jour des systèmes FortiOS sans interrompre le service rendu aux utilisateurs. Le nouveau firmware est d'abord déployé sur les nœuds secondaires puis un device failover est déclenché (son délai de convergence peut-être inférieur à la seconde) au profit d'un nouveau nœud maître. L'ancien est alors mis à jour à son tour. Le cluster reprend alors sa configuration nominale (requiert que le nœud maître soit prélablement configuré pour être préempté lorsqu'il redevient actif).

Bien qu'un cluster soit considéré comme un équipement unique, chaque nœud qui le constitue, peuvent être contrôlé (prise de contrôle à distance en CLI ou GUI) par le biais d'une interface dédiée totalement étrangère au mécanisme de haute disponibilité.

Lorsque les nœuds hébergent des vdoms, la fonction de virtual cluster (restreinte à un cluster de deux nœuds) réalise un partage de charge sur un cluster en mode A-P. Ainsi les ressources physiques du nœud secondaire sont pleinement exploitées au lieu d'attendre une éventuelle défaillance du maître.



L'autre moyen permettant la mise en œuvre de clusters dont tous les nœuds traitent du trafic est d'utiliser le mode A-A. Le nœud maître peut alors utiliser un algorithme de partage (round robin, weighted round robin, random, ip ou port, etc.) distribuant la charge sur les autres nœuds. Lorsque les équipements sont munis de l'ASIC FortiASIC Network Processor, le trafic redirigé est accéléré si bien que les ressources CPU du maître ne sont plus sollicitées pour les sessions établies.

FGCP permet de couvrir trois types de défaillance pouvant survenir durant la vie d'une plateforme :

- Device failover : protège contre la perte totale du nœud primaire. FGCP et son mécanisme de surveillance hearbeat permet de couvrir un dysfonctionnement du nœud maître. Lorsque les nœuds secondaires ne voient plus les messages heartbeat provenant du maître, ils démarrent un processus d'élection visant à identifier le nouveau nœud maître.

- Link failover : protège contre la perte de lien d'une interface physique du nœud primaire. Lorsqu'un nœud détecte la perte de lien (link down) d'une interface surveillée, il propage cet incident à tous les autres nœuds du cluster. La règle est que le nœud ayant le plus d'interfaces surveillées en état opérationnel soit le maître.

- Remote link failover : protège contre la perte d'un lien sur le chemin employé par les flux de production. La fonction ping server ou TCP/UDP echo est utilisée pour détecter la perte d'un équipement ou d'un lien sur le chemin que doit emprunter le flux de production.

La durée de la bascule, c'est-à-dire le temps de convergence du service en état opérationnel est généralement de quelques secondes. Certains critères peuvent avoir une incidence sur ce délai : l'agrégation d'interfaces physiques, la durée de prise en compte des pertes de liens par les commutateurs adjacents, la latence du réseau, etc.

Afin de minimiser l'impact d'une bascule sur le service, Fortinet a développé une technologie permettant de réaliser une convergence en moins de 1 seconde (subsecond failover). Elle s'applique pour le device et le link failover.

Pour que le service soit efficacement restauré au terme de la convergence, il ne faut éviter que les sessions déjà autorisées ne soit recréées par les utilisateurs. C'est pourquoi, la haute disponibilité de FortiOS propose la synchronisation des sessions mais également des baux DHCP, des associations de phase 2 IKE, les tables de routages, etc.

Accès et Authentification

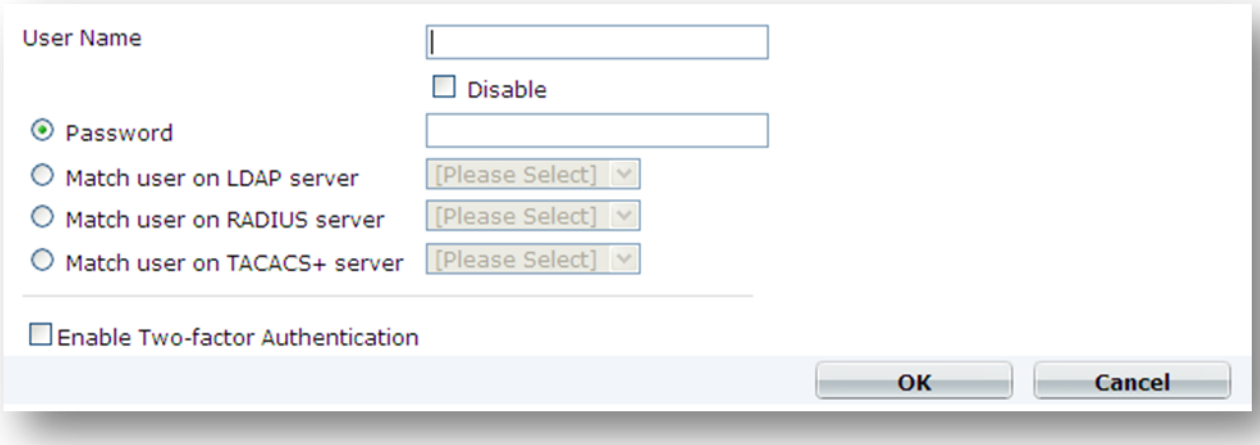
L'usurpation d'identité est l'une des attaques les plus classiques et donc des plus répandues. FortiOS intègre de multiples solutions d'authentification afin d'offrir une grande flexibilité et un maximum de sécurité.

Serveurs d'authentification distante

Pour les utilisateurs qui ne souhaitent pas configurer un serveur distant, il est possible de créer plusieurs comptes locaux stockés sur la mémoire flash.

Dans le cadre de l'utilisation des serveurs d'authentification, le fortiOS supporte les connexions vers :

- les serveurs LDAP : après configuration des paramètres de base, il est possible de lancer une requête pour découvrir le dn et l'architecture du serveur ldap. La connexion vers le serveur peut être sécurisée, les méthodes de connexion au serveur sont « anonyme, régulière ou simple ».
- les serveurs RADIUS : pour chaque serveur déclaré, un backup peut être ajouté en cas de problème sur un des équipements. Les protocoles d'authentification supportés sont PAP, CHAP, MS-CHAP, MS-CHAPv2.
- les serveurs TACACS+ : les types d'authentification supportés sont auto, ASCII, CHAP, PAP, MSCHAP.



Interface de création d'un utilisateur

Les utilisateurs doivent être ajoutés à un ou plusieurs groupes dont le type peut différer :

- Type firewall : sert à forcer un utilisateur à s'authentifier avant de pouvoir établir une session au travers du firewall (prompt).
- Type SSLVPN : sert à authentifier les clients SSLVPN et à définir les paramètres de fonctionnement du VPN.
- Type Active Directory : sert à authentifier les utilisateurs à partir d'un serveur Active Directory en utilisant le logiciel FSSO. L'authentification semble transparente aux yeux des utilisateurs qui s'authentifient sur le pare-feu en même temps qu'ils le font sur leur poste de travail. Voir section suivante.

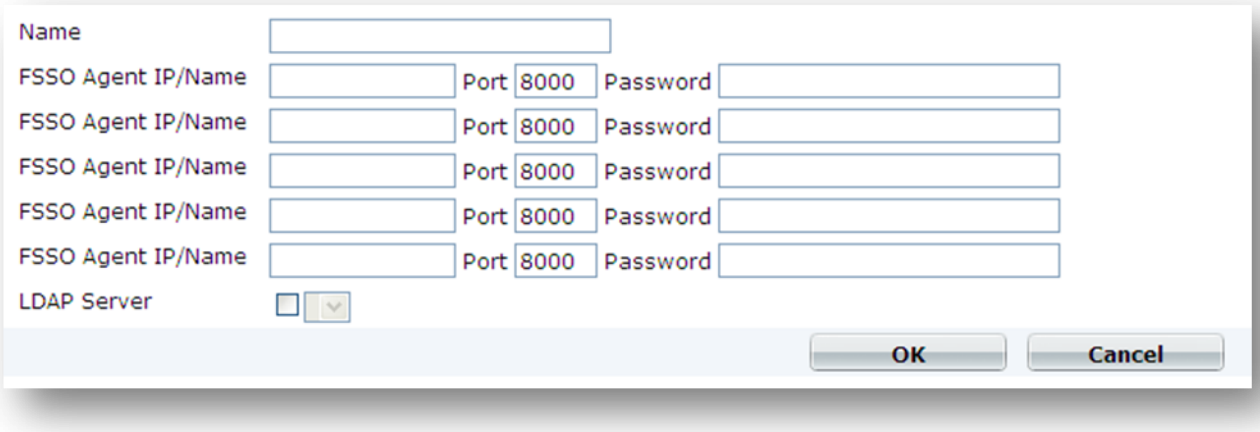
Authentification transparente

L'authentification transparente est possible avec l'utilisation conjointe d'un logiciel FSSO fourni par Fortinet. Trois configurations sont possibles selon les besoins des clients :

- Le client peut installer le logiciel FSSO sur les serveurs qui contrôlent son domaine ainsi que le « collecteur Agent » sur un serveur pilote. Dans ce cas, l'authentification d'un utilisateur sur son poste est immédiatement détectée par le logiciel FSSO puis centralisée par le collecteur agent qui communique les précieuses informations au pare-feu.
- Le client ne souhaite pas installer le logiciel FSSO sur tous ses serveurs. Dans ce cas, il peut installer le logiciel FSSO sur un seul serveur et configurer l'authentification NTLM sur son navigateur. Le navigateur transmettra le couple (utilisateur, mot de passe) lors de

la connexion au travers du pare-feu qui vérifiera ensuite l'authentification sur le serveur AD correspondant.

- Le client ne souhaite pas installer de logiciel sur aucun de ses serveurs AD. Dans ce cas, le mode « polling » du logiciel FSSO peut être utilisé sur un serveur quelconque faisant partie du domaine. Le logiciel utilise les journaux d'authentification présents sur les serveurs AD afin de maintenir ses tables d'authentification à jour.



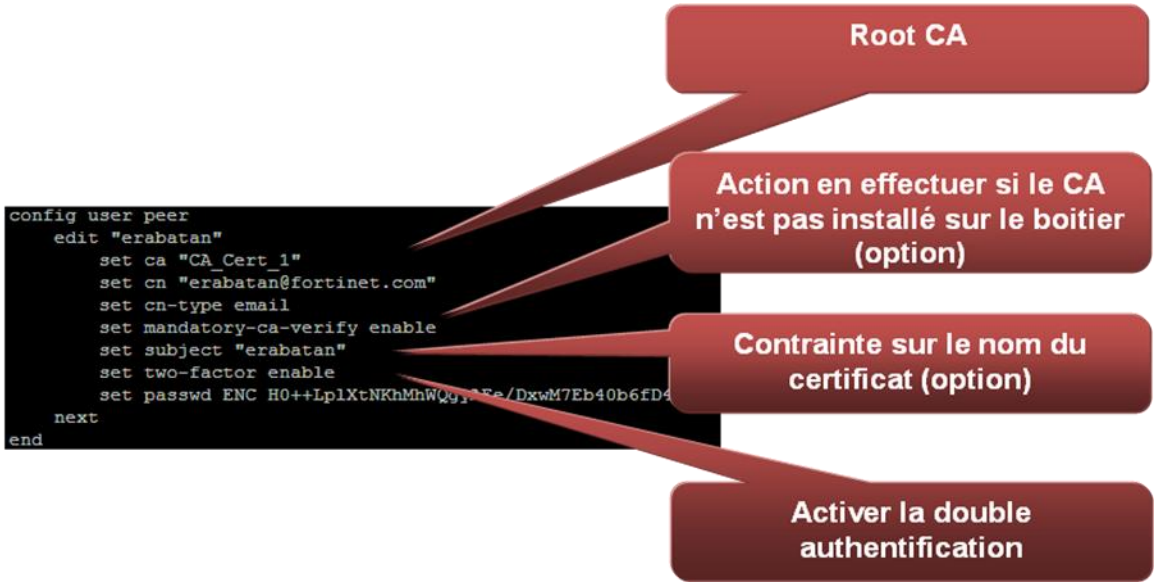
Configuration de la FSSO

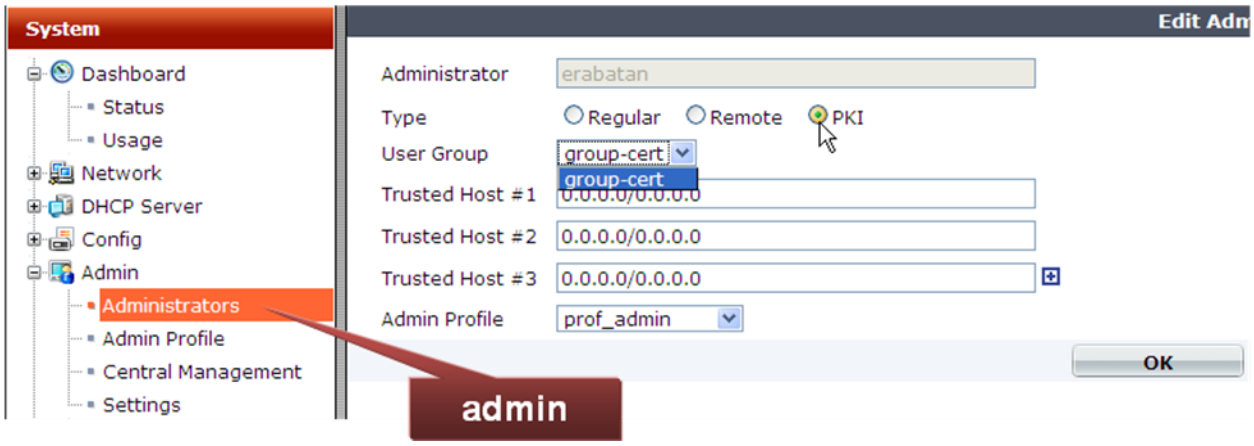
Pour davantage d'informations sur l'installation et la configuration du module FSSO, consulter le « FSSO Technical Note » à l'adresse : http://docs.forticare.com/fgt.html .

Authentification PKI

Ce procédé d'authentification permet d'atteindre directement l'interface d'administration du pare-feu, du portail VPN SSL ou d'authentifier son client VPN IPSec nomade sans passer par le portail d'authentification. Ceci est réalisé par un échange de certificats entre le navigateur du poste client et la fortigate. Pour ce faire, le certificat présent sur le poste client doit avoir été signé au préalable par une autorité de certification dont le root CA a été installé sur le pare-feu.

Une double authentification (certificat puis mot de passe) peut être requise par l'administrateur depuis la CLI :





D'autre part le fortiOS supporte les déploiements automatisés des certificats via le protocole SCEP ou la création et l'import de listes de révocation de certificats (CRL) pour une gestion dynamique des authentifications.

Le fortiOS permet de générer une demande de certificats ou d'importer des certificats au format PKCS12 pour déporter l'authentification d'un serveur sur le fortiGate par exemple.

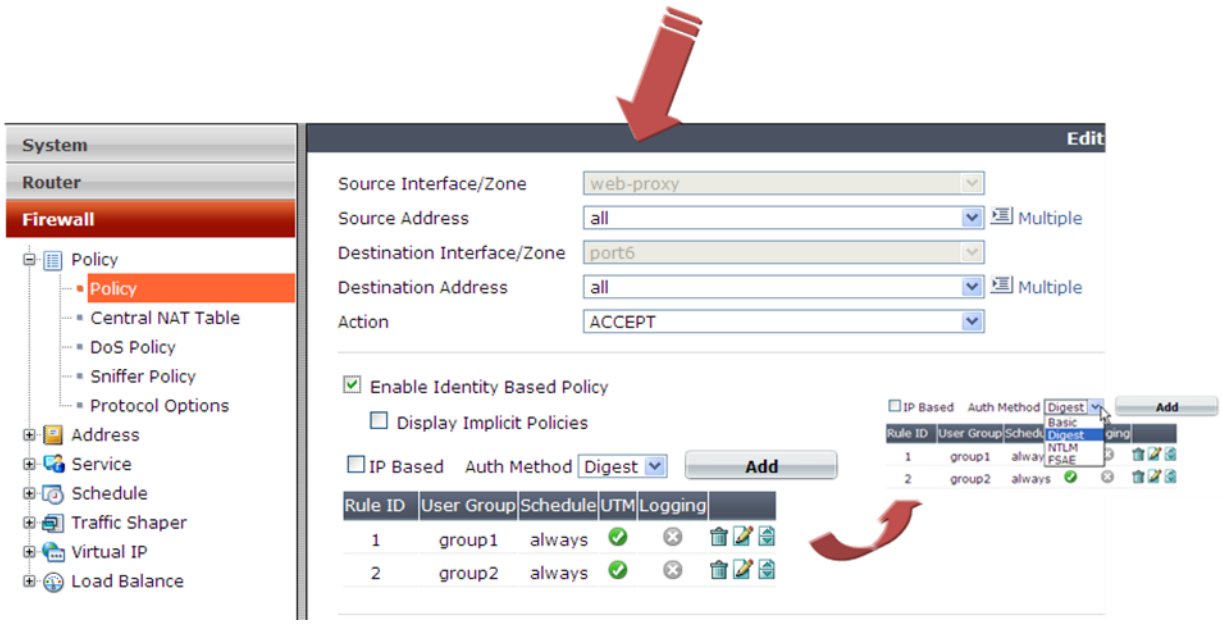
La nouvelle approche IPB et l'authentification par sessions

La version 4.0 introduit les règles de pare-feu basées sur les groupes d'authentifications plus que sur les ip sources et ip destinations qui les caractérisent généralement. Ainsi est il possible d'associer une règle de pare-feu et chacun de ses paramètres (service, calendrier, lissage du trafic, application, …) à un utilisateur ou groupe d'utilisateurs quels que soient leurs types.

Lors de la tentative d'association d'un flux à une règle de pare-feu, un échec de l'authentification entraine une vérification sur le groupe d'authentification suivante. Ainsi est-il possible de restreindre un groupe d'utilisateurs à l'emploi de certaines applications, un calendrier, un lissage du trafic ou avec tous les autres paramètres qui composent les règles de pare-feu.

La nouvelle approche IPB simplifie la conception des règles de pare-feu impliquant des groupes d'authentifications sans altérer les possibilités offertes.

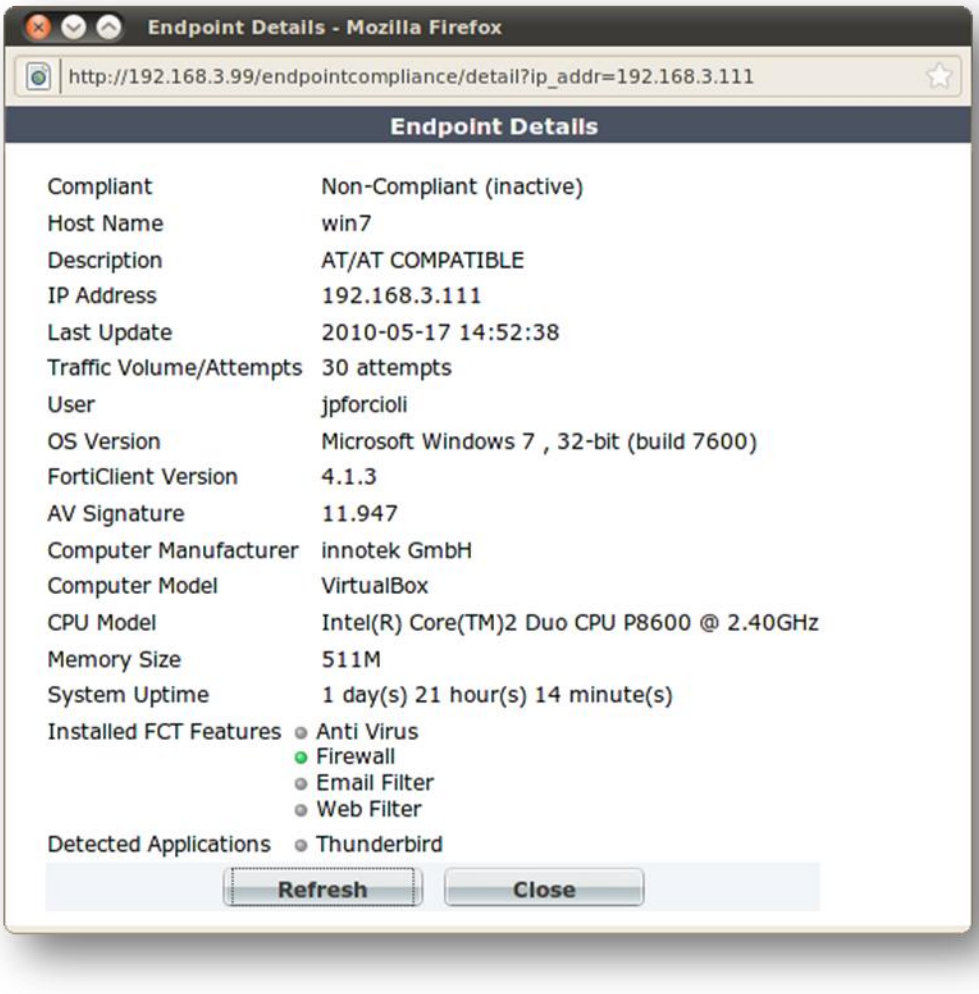
Dans le cadre de l'utilisation d'un proxy web ou d'une plateforme mutualisée à partir de laquelle plusieurs utilisateurs peuvent créer des connexions, le pare-feu voit plusieurs sessions provenant de la même source (adresse ip). L'authentification par ip source classique ne suffit donc pas à authentifier plusieurs utilisateurs appartenant à des groupes différents avec des profiles de filtrage différents. La nouvelle approche IBP facilite la configuration de l'authentification par session introduite en v.4.2. Conjointe à l'utilisation du proxy explicite du FortiOS, l'authentification par session est véhiculée par le protocole http (authentification basic, digest ou transparente) au travers du navigateur. Ainsi chaque session ouverte par le navigateur est considérée comme unique par le pare-feu qui contrôle les paramètres d'authentifications véhiculés.



Authentification par session en utilisant la méthode digest

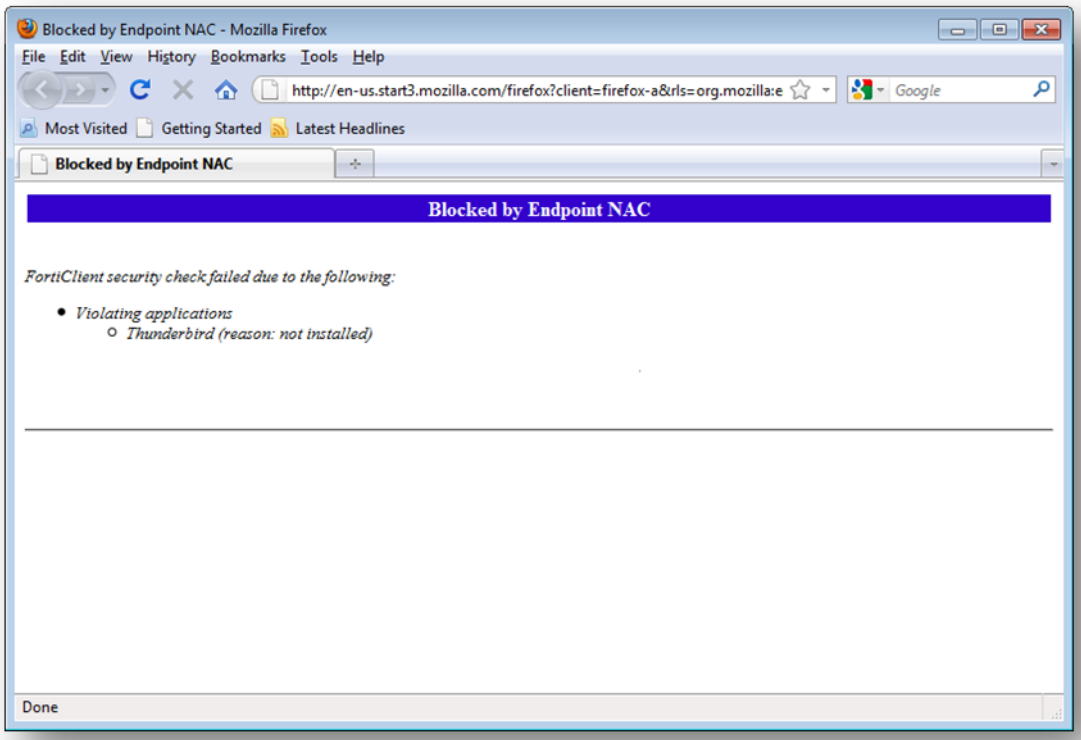
Endpoint Control

La fonctionnalité d'Endpoint Control vient renforcer l'utilisation du FortiClient sur les postes clients qui ouvrent des connexions au travers du pare-feu. Cette fonctionnalité garantit à l'administrateur du réseau que les connexions créées proviennent de postes utilisant les dernières versions du Forticlient, avec des signatures à jour, un pare-feu activé ou embarquant uniquement des applications validées au préalable. Plus de 2000 applications sont reconnues qu'elles soient actives, simplement installées ou non installées sur le poste.



Informations livrées par le fortiClient au fortiGate par le module Endpoint Control

Dans le cas ou un poste ne satisfait pas la politique de sécurité exigée, le fortiOS peut rediriger la session vers le portail de téléchargement du Forticlient, vers une page justificative de cette non-conformité ou peut autoriser et tracer la session.



Poste bloqué car il ne dispose pas de l'application « thunderbird »

Administration

Les produits de la gamme Fortigate proposent plusieurs méthodes d'administration et de supervision. Pour l'administration, celle-ci peut-être réalisée directement sur l'équipement lui-même (administration locale) ou via un équipement de gestion centralisé : le FortiManager. En ce qui concerne l'administration locale, celle-ci peut être effectuée à l'aide d'une interface graphique élaborée et sans client lourd (utilisation d'un navigateur standard) ou en ligne de commande. Cette dernière méthode offre ainsi la possibilité de réaliser les tâches courantes d'administration à travers des scripts et de pouvoir de cette manière automatiser certains processus.

Administration locale

L'accès à l'équipement est nécessairement sécurisé au travers de comptes d'administration et de profils associés. Les comptes définissent les informations de connexion de l'administrateur. A ce titre le compte peut être 'local', c'est à dire qu'il est propre à l'équipement et configurer directement sur celui-ci ou bien externe, dans ce cas l'équipement est en liaison avec une base d'authentification externe (ldap, RADIUS, TACACS+, PKI, ...) qui centralise l'ensemble des compte d'administration y compris pour des équipements tiers.

Outre la notion d'identification des administrateurs, il est également possible de restreindre l'accès à l'équipement uniquement à partir de machines ou de sous-réseaux identifiés (notion d'hôtes ou de réseaux de confiance).

Chaque compte d'administration est associé à un *profil*. Les profils définissent les domaines et niveaux d'accès de chaque administrateur, ainsi il est possible d'ajuster les droits en lecture ou écriture en fonction des parties de configuration à visualiser ou modifier. Un administrateur est identifié puis associé à son profil de protection au moment où il s'authentifie sur le portail d'accès.

Administration centralisée

La solution d'administration centralisée des appliances Fortinet est composée des équipements FortiManager et FortiAnalyzer.

1. FortiManager

L'appliance FortiManager offre une interface WebUI d'administration centralisée des équipements FortiNet (FortiGate, FortiAnalyzer, FortiMail et FortiClient) reposant sur la technologie AJAX pour renforcer l'expérience utilisateur. FortiManager intègre de nombreuses fonctionnalités incluant :

La virtualisation

Un équipement FortiManager peut être virtualisé de manière à proposer plusieurs instances d'administration. Chacune d'elles gère un parc d'équipements Fortinet. Une instance virtuelle est nommée Administrative Domain ou adom.

Haute disponibilité

FortiManager intègre un mécanisme de haute disponibilité permet de synchroniser jusqu'à six équipements.

Il repose sur un protocole L3 utilisant les adresses des équipements et un protocole sécurisé par SSL opérant sur le port 5199/tcp. Il véhicule les messages de surveillance heartbeat ainsi que les flux de synchronisation.

La priorité de ce mécanisme de HA est de synchroniser l'ensemble des informations entre tous les membres participants. En cas de défaillance, afin de s'assurer que les équipements administrés vont utiliser un FortiManager parfaitement synchronisé, la bascule est réalisée manuellement par un administrateur. Il y a deux scénarios possibles :

- Le FortiManager maître est inopérant : un trap snmp ainsi qu'un log est continuellement envoyé par les équipements secondaires pour avertir l'administrateur du dysfonctionnement. L'équipement maître est retiré de la configuration des équipements secondaires et un nouveau membre maître est désigné par l'administrateur (requiert une réinitialisation de l'équipement).

- Un des FortiManager secondaire est inopérant : un trap snmp ainsi qu'un log est continuellement envoyé par les autres équipements pour avertir l'administrateur du dysfonctionnement. L'équipement doit être sorti manuellement du cluster afin de ne pas risque une pollution des bases dans l'hypothèse ou il redeviendrait soudainement fonctionnel.

Dans tous les cas, l'administrateur est informé par trap ou log. Il doit modifier la configuration du cluster sur chaque membre et le cas échéant désigner un nouveau membre maître.

Les équipements administrés (FortiGate, FortiAnalyzer, FortiMail, etc) doivent quant à eux déclarer préalablement la liste des FortiManager susceptibles d'être utilisés. Un mécanisme de polling permet d'assurer que seul le FortiManager maître est utilisé.

La mise à jour d'un cluster de FortiManager est automatisée et provoque l'interruption momentanée du service. Le nouveau firmware est tout d'abord installé sur le membre maître avant d'être déployé sur les autres membres.

Droits d'administration

L'authentification des administrateurs peut-être réalisée par le FortiManager (base locale) ou par un serveur Radius/Tacacs.

Un administrateur est associé à un adom et à un profil d'administration définissant les autorisations d'accès aux modules fonctionnels de l'interface WebUI.

Par exemple, un administrateur ne disposant d'aucun droit d'écriture peut être déclaré sur l'équipement à des fins d'audits.

A noter que pour protéger la base de données des accès concurrents sur le même équipement, un mécanisme de verrou est mis en œuvre. Lorsque le verrou est activé, un administrateur est averti qu'il ne peut pas réaliser de changement lorsqu'il tente de modifier la configuration d'un équipement verrouillé.

Protocole FMFG

Le protocole FMFG prend en charge la communication du FortiManager avec les équipements administrés. Il est sécurisé par SSL/TLS et tourne sur le port 541/tcp. Le protocole intègre des mécanismes de découvertes automatique de configuration ainsi que de protection qui évite la mise en état instable d'un équipement si la communication venait a être interrompue brutalement par exemple.

Gestion des changements

FortiManager permet de gérer des équipements en mode hors ligne. Cela permet de planifier les changements et de ne les déployer que lorsque c'est nécessaire. FortiManager offre une interface d'administration similaire au FortiGate si bien que l'administrateur n'est pas dépaysé.

Les changements ne sont appliqués que sur l'invocation explicite d'une installation (bouton Install). Il est possible de limiter la portée des changements à tout ou partie des équipements administrés. L'application peut également est planifiée pour se déclencher automatiquement à une date ultérieure.

Gestion des révisions

Chaque installation instancie une version de configuration qui s'ajoute dans la base de données des configurations. Il est possible de comparer entre-elles différentes versions de configuration en mode diff . Cela peut permettre d'identifier les changements qui auraient pu provoquer des problèmes par exemple.

Une version antérieure de configuration peut être restaurée.

Mise à jour des firmwares

FortiManager maintient automatiquement une base des derniers firmwares correspondant aux équipements administrés. Il est ensuite possible de lancer ou planifier une mise à jour automatisée sur tout ou partie du parc.

Lorsqu'elle est déclenché, une journalisation des tâches permet de suivre l'état d'avancement de l'opération .

Serveur FortiGuard

FortiManager peut servir les mises à jour AV et IPS aux équipements FortiGate administrés. Il opère également les services de catégorisation et d'identification de SPAM. Cette fonction adresse les cas ou les équipements ne peuvent se mettre à jour sur Internet. La fonction propose un tableau de bord indiquant pour chaque équipement les versions de bases utilisées.

Supervision

Le module fonctionnel Real Time Monitor autorise la mise en place d'une supervision du parc d'équipements administrés. Il repose sur le protocole SNMP aussi bien pour la réception de trap que pour l'interrogation d'OID. Il se présente sous la forme d'onglets dont le nombre ainsi que le contenu sont personnalisables.

Des widgets peuvent être crées pour surveiller des indicateurs SNMP. Il est également possible de définir des seuils qui une fois dépassés provoquent l'envoie d'alertes mails.

VPN Manager

Ce module adresse la problématique d'une combinatoire exponentielle lorsqu'un volume conséquent d'équipements administrés doivent constituer des topologies de tunnels IPSEC fortement maillée ou en étoile.

Il prend en entrée, les paramètres IKE de phase 1 et 2, la liste des équipements participants et la topologie du VPN. Il provisionne alors automatiquement les éléments de configuration requis sur chaque équipement.

2. FortiAnalyzer

L'appliance FortiAnalyzer reçoit les événements (logs), stocke et produit les rapports statistics des équipements administrés.

Stockage

Les logs sont hébergés sur l'espace de stockage présent sur l'appliance. En fonction de la gamme, certains niveau de RAID peuvent être mis en place. Le niveau est fonction du critère à privilégier (performance/redondance).

Chaque équipement FortiGate susceptible d'envoyer des logs doit être préalablement déclaré. Cela permet d'associer un quota de stockage personnalisé. Un tableau de bord permet de consulter visuellement l'état du quota de tous les équipements.

FortiAnalyzer propose un mécanisme de permutation de journaux utilisant le volume ou une fréquence temporelle comme déclencheur. Il est possible d'automatiser la sauvegarde automatique d'un journal vers un serveur tiers, ainsi que sa suppression de l'espace de stockage.

FortiAnalyzer propose également un stockage dans une base de données SQL interne ou distante (MySQL). Cela procure l'avantage de créer des indicateurs de rapports personnalisés. Cela permet également d'augmenter la capacité de stockage qui est déportée sur le serveur de base de données.

Consultation des journaux

L'interface de consultation des journaux propose un moteur de recherche simple qui peut être déclinée afin de réaliser une recherche avancée. FortiaAnalyzer privilégie la réactivité en affichant les résultats dès qu'ils comment à être obtenus tout en continuant à charger le reste en arrière plan présenté par un affichage multipage. Un état d'avancement (en %) de la restitution des résultats est continuellement présenté à l'utilisateur. Un bouton « stop » permet d'interrompre une recherche.

FortiAnalyzer propose une fonction nommée eDiscovery permettant de sauvegarder le résultat d'une recherche dans un répertoire virtuel.

Enfin, il est possible de parcourir les journaux séparément par équipement et par type (attack, traffic, event, etc.).

Reporting

FortiAnalyzer propose un moteur de reporting à la fois simple et complet permettant la génération automatisée de rapports dont le contenu est adapté au profil de leur destinateur (opérationnel, sécurité, direction, etc.).

Un rapport est créé à partir d'un profil de mise en page, d'une source de données et d'un format de sortie à produire.

- Mise en page : elle permet de contrôler l'apparence du rapport qui sera généré. Un certains nombres d'éléments sont paramétrables : titre, logo, indicateurs à incorporer et texte d'informations.
- FortiAnalyzer propose une centaine d'indicateurs prédéfinis couvrant différents domaine : réseau, sécurité, UTM (AV, filtrage d'URL, IPS, DLP), accélération WAN, etc. Chaque indicateur est personnalisable : top N avec N variable, apparence (tableau ou graphe), résolution éventuelle.
- Source de données : la source de données définit le périmètre des logs depuis lequel le rapport sera généré. Elle n'est pas obligatoire car par défaut, FortiAnalyzer travaille sur un équipement et une plage temporelle. Toutefois il est possible d'affiner la portée d'analyse en ne sélectionnant que certains logs filtrés par d'autres critères. La granularité peut aller jusqu'à n'importe quel champ d'un log.
- Format de sortie : les formats HTML, PDF, TXT, MHT et XML sont supportés.

Les rapports sont générés à la demande (pratique pour du reporting ponctuel) ou de manière planifiée. Ils peuvent être sauvegardés sur un serveur tiers ou être envoyés à leur destinataire par e-mail.

VPN et protection des données

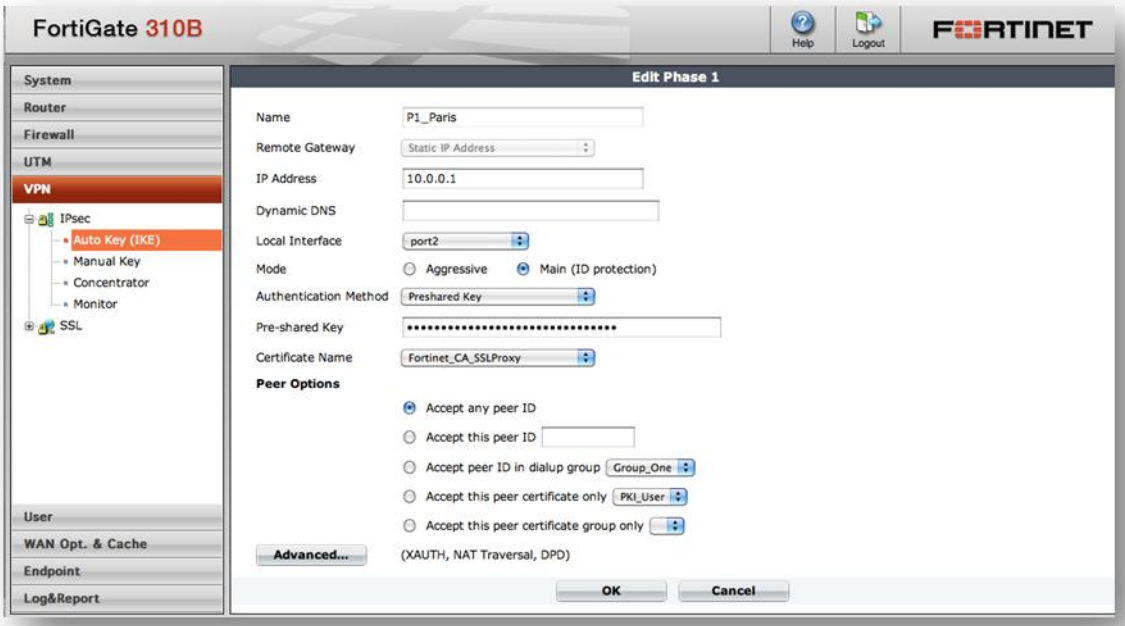
Le fortiOS intègre de manière standard est sans aucun surcoût un ensemble de fonctionnalités permettant de mettre e place des réseaux privés virtuels, de gérer les flux transitant à travers l'équipement via des fonction de gestion de qualité de service, d'administration des communications et d'optimisation des liaisons longue distance (WAN) .

VPN IPSec

FortiOS supporte les tunnels VPN IPSec dont la phase1 est basée sur le protocole IKE (version 1 ou 2) ainsi que les fonctions de 'NAT Traversal' pour la négociation des paramètres du tunnel, l'authentification, la génération des clefs de chiffrement des données et l'établissement du tunnel et le protocole ESP pour la transmission des données (ip-protocol 50). Toutes ces fonctions sont réalisées aux travers des ASIC implantés dans les équipements et bénéficient ainsi de l'accélération matérielle et d'un niveau de performance accru.

Les standards IPSec sont bien entendu respectés tout en conservant une grande souplesse de configuration par le support de différents modes de configuration :

- IKE mode config
- mode Policy server pour les tunnels dialup des utilisateurs nomades
- fourniture automatisée des adresses au travers du tunnel (DHCP over IPSec)



L'authentification du tunnel est réalisée par mot de passe (pre-sharedkey), ou par certificats digitaux. Une authentification utilisateur de type XAUTH (reposant sur les différents référentiels d'utilisateurs supportés par FortiOS) peut être adjointe à celle du tunnel. Le module VPN IPSec permet de configurer les réseaux privés en fonction des contraintes opérationnelles et autorise l'implémentation des différentes topologies rencontrées :

- Site à site : cette architecture permet de relier deux sites distants par un lien public en le sécurisant. Un tunnel est crée entre les deux sites et les données sont encapsulées de l'un à l'autre. Deux clients situés sur deux sites distants peuvent alors communiquer simplement sans aucune modification ou ajout sur aucun des postes. Le type de passerelle distante supportée peut être en adressage IP statique ou en DNS dynamique.

- Maillage complet (full mesh) : il s'agit d'une variante du cas précédent, lorsqu'il y a plus de 2 sites en cause, il est possible de concevoir une architecture où chaque site est connecté à l'ensemble des autres réduisant au minimum l'impact de la perte d'un lien.

- Concentrateur (hub and spoke) : cette architecture est adaptée aux sites multiples également. Un site central établit des liaisons VPN avec plusieurs sites distants qui ne sont pas reliés entre eux. Le site central qui agrège tous les VPN peut servir de concentrateur pour relayer les données d'un site à un autre. Ainsi les sites distants sont virtuellement reliés entre eux. Ainsi, une fois le tunnel VPN monté, deux clients situés sur des réseaux distants peuvent communiquer l'un avec l'autre comme s'ils étaient situés sur le même réseau LAN. Un client peut naviguer sur internet en utilisant la connexion internet du site distant.

- Client à site. Cette architecture permet de relier un client connecté à l'Internet à distance au site principal. Le poste client obtient une adresse virtuelle qui peut faire partie du LAN protégé par la passerelle simulant ainsi virtuellement sa place sur le LAN. La phase1 doit être configurée avec le type 'utilisateur dialup' car l'adresse IP du client n'est pas connue la plupart du temps. Un client Dialup peut naviguer sur internet en utilisant le filtrage du Fortigate.

Il est possible d'utiliser deux méthodes de configuration pour l'implémentation des tunnels au sein des équipements : un mode basé sur les règles de pare-feu (Policy based) et un mode interface (route based). Les différences principales entre les deux modes sont les suivantes :

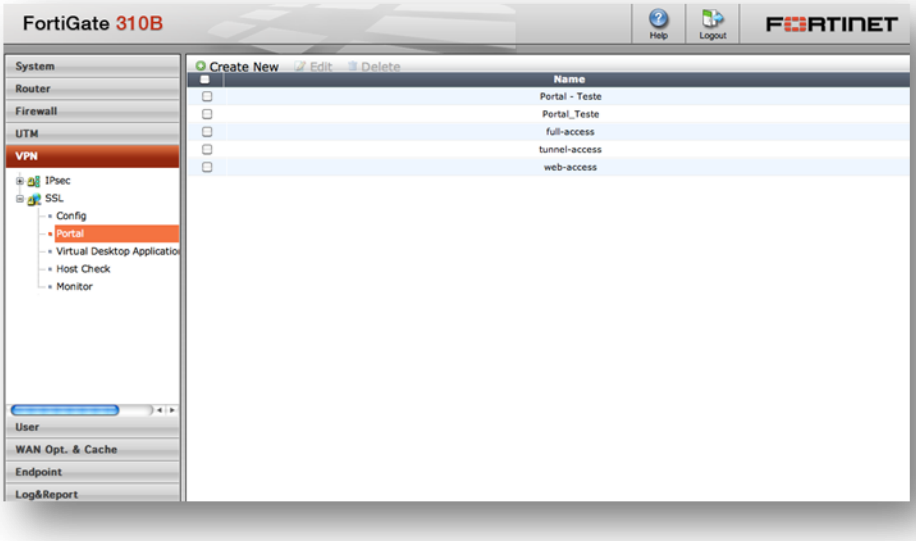
Policy based	Route based
Disponible en mode NAT/route et en mode transparent	Disponible uniquement en mode NAT/route
Nécessite une règle de pare-feu avec unbe action IPSEC qui spécifie le tunnel, une règle contrôle les connexions dans les deux sens	Nécessite uniquement une règle de pare-feu simple avec une action ACCEPT. Une règle est nécessaire pour autoriser l'initiation des sessions dans chaque sens de communication
Ne supporte pas les protocoles de routage dynamique	Supporte le routage dynamique le tunnel étant géré comme une interface

VPN SSL

Le FortiOS intègre en standard et sans coût supplémentaire la fonction VPN SSL. Elle se décline en deux modes distincts et non exclusifs : le mode web et le mode tunnel. En mode web tous les flux sont encapsulés dans un flux SSL ne nécessitant ainsi qu'un navigateur web afin d'initier et d'utiliser le réseau privé virtuel ainsi constitué. Dans ce mode les données ne sont pas encapsulées dans un tunnel mais reposent uniquement sur le protocole https sécurisé par la couche SSL. De ce fait, certaines applications non compatibles avec le protocole http ne peuvent pas fonctionner. Dans ce cas, le portail SSL prend le relais qui assure la redirection et l'encapsulation. Les flux supportés par cette méthode sont : http, https, ftp, rdp, smb/cifs, ssh, telnet, vnc et ping. L'application permettant la connexion distante sur le portail étant un navigateur, ce mode est indépendant du système d'exploitation et de la plate-forme matérielle utilisée.

Le mode tunnel, n'impose aucune restriction sur les applications utilisables à travers le lien sécurisé puisque l'ensemble du trafic émis par le poste client est encapsulé dans le tunnel SSL

avant d'être remis en clair par le boîtier Fortigate. Une pile IP virtuelle chiffrant tout le trafic est utilisée nécessitant l'installation d'un client sur le poste nomade, celui-ci peut généralement être téléchargé directement à partir du portail d'accès, il nécessite en revanche de disposer des droits d'administration locaux sur le poste. Ce mode fonctionne avec l'attribution d'une adresse IP spécifique au client. Afin de facilité l'administration du tunnel, une interface virtuelle est créée. Une route statique ajoutée sur l'interface virtuelle destination du client permet une communication d'un client VPN SSL en mode tunnel à un autre, l'établissement d'une session depuis un client sur le LAN vers un client rattaché au réseau par un tunnel VPN SSL. La navigation sur l'Internet depuis un client VPN SSL passe par défaut par le boîtier ce qui permet de profiter des fonctionnalités de filtrage offertes par le celui-ci. Ceci étant, il est possible de segmenter le routage (fonction de split-tunneling) et dans ce cas un poste connecté à l'Internet et au réseau de l'entreprise via une connexion VPN SSL peut atteindre l'Internet directement. Dans ce cas, seuls les flux à destination du réseau de l'entreprise sont dirigés dans le tunnel.

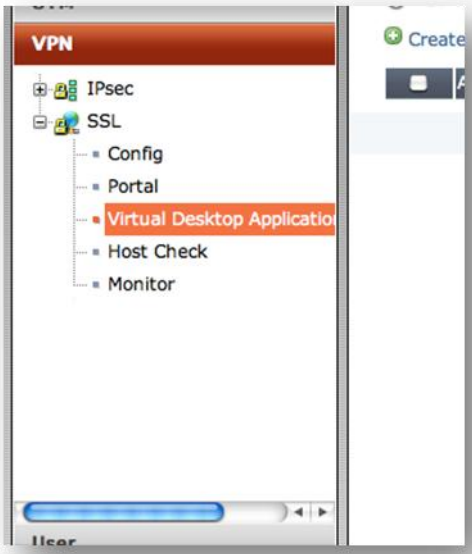


Le mode tunnel nécessite l'utilisation d'un client du coté du poste nomade, celui-ci peut généralement être téléchargé directement à partir du portail d'accès, il nécessite en revanche de disposer des droits d'administration locaux sur le poste. Ce mode permettant l'encapsulation des flux directement à partir du poste nomade, il n'y a pas de restriction quant aux types de flux supportés.

Protection des données

L'accès au réseau de l'entreprise pouvant se faire à partir de points de connexion voire même de postes non maîtrisés par l'entreprise, des fonctions spécifiques permettent de garantir la confidentialité des données échangées après la déconnexion du réseau privé virtuel SSL (cas d'un

accès à partir d'un hôtel ou d'un cyber-café). Il est ainsi possible de forcer le nettoyage du cache du navigateur lors de la déconnexion ou la rupture de communication. Il est également possible d'effectuer toutes les opérations durant la connexion en VPN SSL dans un bureau virtuel (application fonctionnant sur le poste distant), lors de la déconnexion cette application est arrêtée et toutes les données associées à la connexion disparaissent définitivement, ne laissant aucunes traces sur le poste. Pour plus de confidentialité, il est également possible de masquer aux yeux de l'utilisateur, l'adresse réelle de la ressource qu'il essaie d'atteindre via l'option de masquage d'adresse (URL obfuscation).



Validation du poste distant

Toujours afin d'assurer le meilleur niveau de protection des informations et du réseau interne, outre l'authentification de l'utilisateur lui-même, des fonctions de vérification du poste distant sont disponibles au sein du module VPN SSL. Ces fonctions permettent de vérifier que le poste distant est conforme à certaines règles de sécurité en accord avec la politique interne : dispose d'un anti-virus à jour, dispose d'un pare-feu...

VPN L2TP

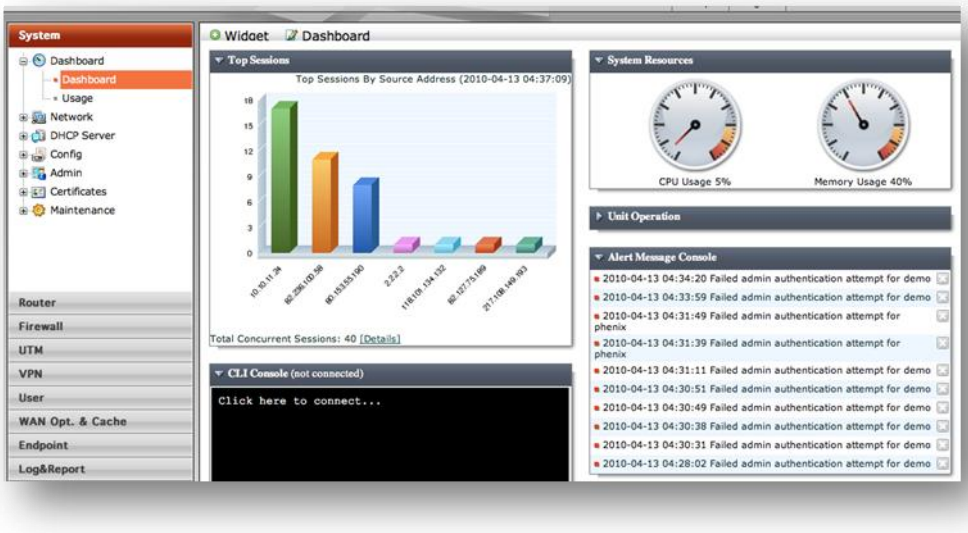
FortiOS supporte L2TP et permet la connexion de clients distants utilisant cette fonction. La méthode de chiffrement supportée est MPPE (Microsoft Point to Point Encryption).

Lorsqu'un client distant se connecte, une adresse IP d'un intervalle prédéfini et configurable lui est assignée. De plus le client doit s'authentifier à travers les mécanismes de gestion des utilisateurs et des droits par groupe.

Supervision et reporting

Supervision par le tableau de bord

Plusieurs possibilités sont offertes avec de superviser les équipements. L'équipement lui même fournit un tableau de bord qui est affiché lors de la connexion sur l'interface graphique. Celui-ci est personnalisable tant en ce qui concerne le type d'information affiché que la disposition de l'affichage.



Aperçu du tableau de bord et ses widgets

Supervision SNMP

L'agent SNMP des équipements FortiGate supporte aussi bien les MIB propriétaires Fortinet que les MIB standards (RFC1213 et 2665) Le support des RFC porte sur la partie des MIB 2665 et 1213 qui s'applique aux équipements. Il existe deux fichier MIB propriétaire qui s'applique aux équipements FortiGate : la MIB Fortinet et la MIB FortiGate. La MIB Fortinet contient les traps, champs et informations qui sont communs à tous les produits de la marque Fortinet. La MIB FortiGate contient les traps, champs et informations qui ne portent que sur les FortiGate.

Les gestionnaires SNMP disposent la plupart du temps d'une base de MIB qui intègre en standard les MIB propres aux RFC, en revanche il sera probablement nécessaire d'ajouter les MIB propriétaires Fortinet et FortiGate afin de superviser au mieux ces équipements.

Le tableau suivant indique pour chaque MIB supportée le périmètre couvert.

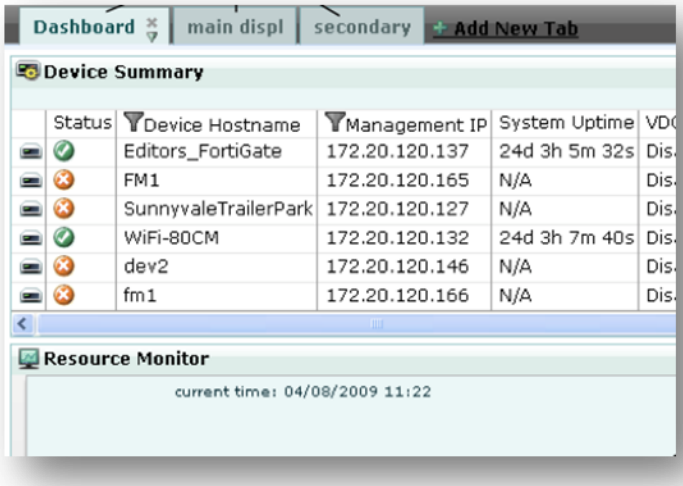
MIB	Description
FORTINET-CORE-MIB.mib	La MIB propriétaire Fortinet intègre toute les informations de configuration du système et les traps qui sont communs à tous les équipements Fortinet. Le gestionnaire SNMP doit disposer de ces informations pour superviser les équipements FortiGate et pour recevoir les traps en provenance de l'agent SNMP de l'équipement.
FORTINET-FORTIGATE-MIB.mib	La MIB propriétaire FortiGate intègre toutes les informations de configuration système et de traps qui sont spécifiques aux équipementsFortiGate. Le gestionnaire SNMP doit disposer de ces informations pour superviser les informations spécifiques à l'équipement (nombre de sessions, état des tunnels VPN, ...)
RFC-1213 (MIB II)	L'agent SNMP des équipements FortiGate support les groupe de la MIB II avec les exceptions suivantes : ▪ groupe EGP (RFC 1213 section 3.11 et 6.10) ▪ les statistiques protocolaires retournées par les groupes de la MIB II (IP /ICMP/TCP/UDP, etc) ne sont pas rigoureusement exactes, celles obtenues à partir de la MIB Fortinet le sont.
RFC-2665 (Ethernet-like MIB)	L'agent SNMP des équipements FortiGate supporte les informations de la MIB Ethernet-like sauf en ce qui concerne les groupes dot3tests et dot3Errors.

Supervision via FortiManager

Le FortiManager permet d'assurer la supervision des équipements gérés à travers son module de surveillance temps réel (RTM : Real Time Monitor). Ce module apporte une vue synthétique sur les équipements, les tendances, les problèmes et les événements qui méritent attention. Plutôt que de suivre chaque équipement en se connectant directement sur celui-ci, le module RTM apporte une vue synthétique de l'ensemble du parc géré. Le FortiManager collecte via SNMP (traps et variables) pour chaque équipement des informations sur l'état de fonctionnement et permet de les visualiser de manière simple.

Les deux parties principales du module RTM sont les notifications et les tableaux de bord. Les notifications informent l'administrateur qu'un événement important est survenu ou qu'une

variable a dépassé un seuil prédéfini (par exemple : disque dure rempli à 80% ou température hors limites). Les tableaux de bord permettent de visualiser et de suivre l'évolution des valeurs de variables surveillées selon différents types de représentations personnalisables.



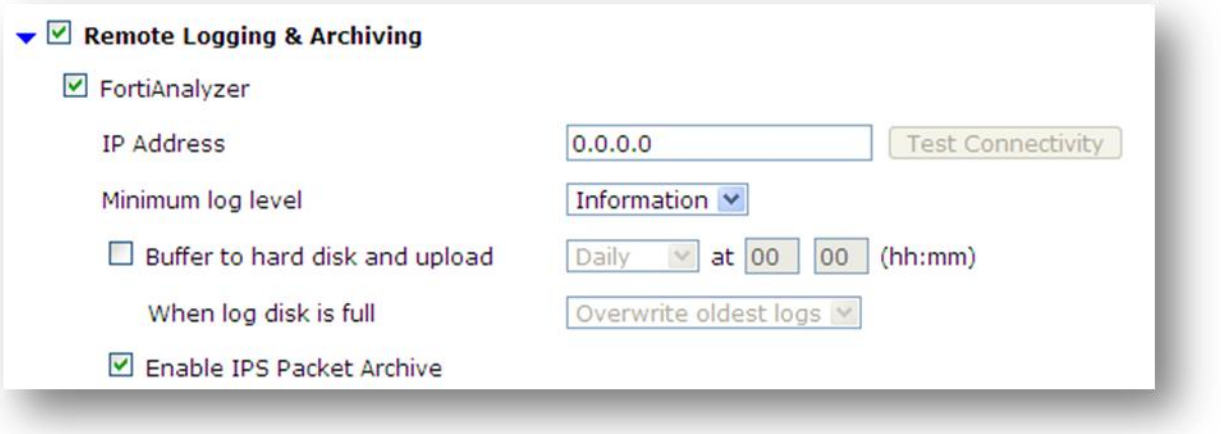
Supervision FortiManager

Supports de Logs

Chacun des boitiers peut émettre des logs au format standard syslog (UDP ou TCP port 514) ou au format SQL depuis la version 4.0 sur la plupart des modèles disposant d'un disque dur.

Les logs peuvent être envoyés à six destinations différentes à la fois parmi des serveurs syslog, un serveur webtrends, plusieurs FortiAnalyzer, le disque dur local du boitier et/ou sa mémoire interne. Pour chacune de ces destinations, il est possible de configurer le seuil de sévérité ainsi que le type de logs (Antivirus, IPS, trafic, évènements systèmes, contrôle applicatif, DLP, antispam, webfilter, network scanning…) qui y seront écrits.

Lorsque le volume de données logguées sur le disque dur local dépasse un seuil, il est possible de recevoir une alerte puis de réécrire sur les logs les plus anciens ou de refuser tout log supplémentaire. Il est également possible d'exporter ses logs sur un serveur ftp, un serveur tftp ou sur un fortiAnalyzer distant.



L'envoi de logs du disque vers le FortiAnalyzer peut être automatisé. Une fois l'export réalisé, l'ensemble des logs restera directement accessible depuis l'interface graphique du boitier via une connection au FortiAnalyzer.

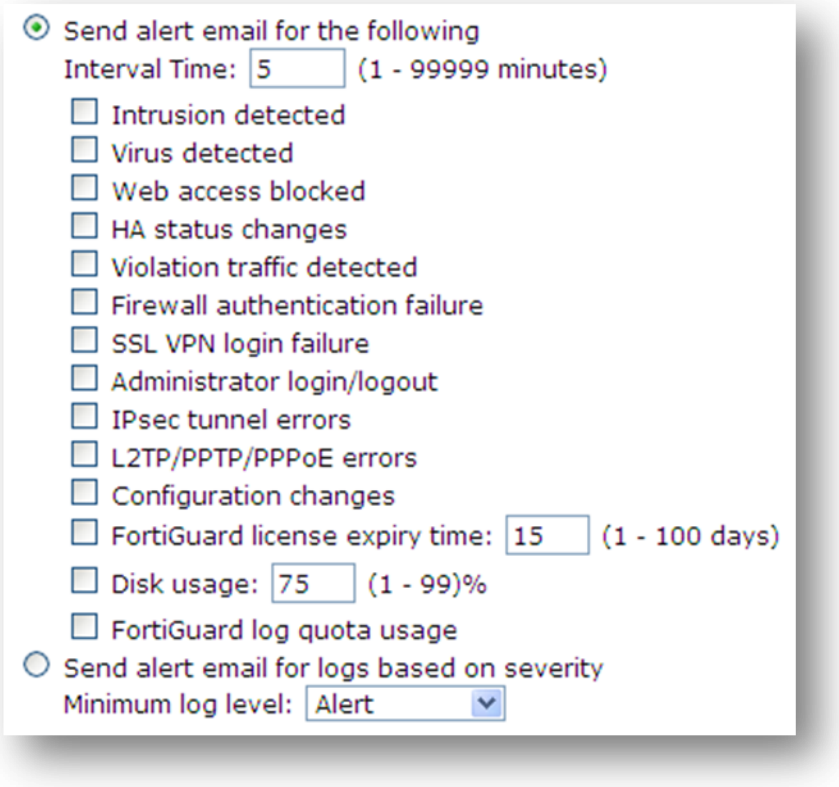
Enfin il est possible de placer en quarantaine sur le disque les éléments détectés par l'analyse DLP (page web, email, conversation d'instant messaging…) ou les paquets ayant provoqué une attaque DOS.

Alertes email

La supervision de logs est un travail quotidien rendu difficile par le nombre d'équipements éventuels à gérer ainsi que le nombre d'évènements potentiels qui susceptibles d'être générés. Aussi l'administrateur peut se simplifier la tâche en configurant des alertes reçues par email lorsqu'un évènement critique survient. Un ou plusieurs comptes emails peuvent être définis avec ou sans authentification sur le serveur SMTP.

Par exemple, il peut définir une limite de volume disque occupé ou un nombre de jours de retard sur le renouvellement de la licence Fortiguard au-delà desquels un email sera envoyé afin de l'avertir de la situation.

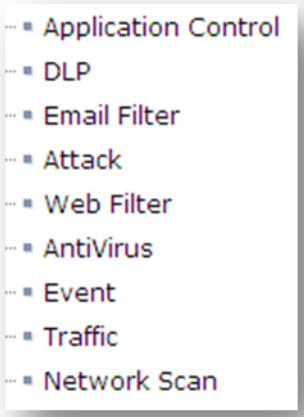
De même une alerte peut être envoyée lorsque plusieurs logs d'une certaine sévérité sont émis dans un intervalle de temps configurable.



Qualité des logs

Les logs du boitier sont disponibles directement depuis la GUI avec un filtre configurable sur chacun des paramètres du log (Ex : date, type, ip source, ip destination, message…) afin de mettre en exergue les informations souhaitées. Le rendu filtré est aussi exportable sous forme de fichier .csv téléchargeable depuis la GUI. Le passage de la souris au dessus d'un log permet de le consulter en totalité dans un tableau pour davantage de clarté.

Chaque évènement lié à l'administration du pare-feu, chaque intervention même quelconque d'un module de filtrage (IPS, AV, Application control, URL Filtering, AS…), ainsi que chaque session peuvent entrainer la génération d'un log dans une catégorie propre.



Les catégories ainsi que les niveaux de logs requis (Debug, Information, Notification, Warning, Error, Critical, Alert, Emergency) sont sélectionnables depuis la GUI et configurables sur chacun des supports de stockage. Ainsi est il possible de stocker sur le disque dur tous les logs de la catégorie traffic pour débogguer une congestion (niveau debug) mais ne conserver que les logs « évènements critiques » sur la mémoire.

Depuis la version 4.1 du fortiOS, les logs peuvent être émis au format SQL sur les équipements disposant d'un disque dur en plus du format syslog habituel. Il est désormais possible :

- D'activer le logging SQL (base SQLite)
- De créer des widgets de rendu d'activité
- De créer et générer des rapports

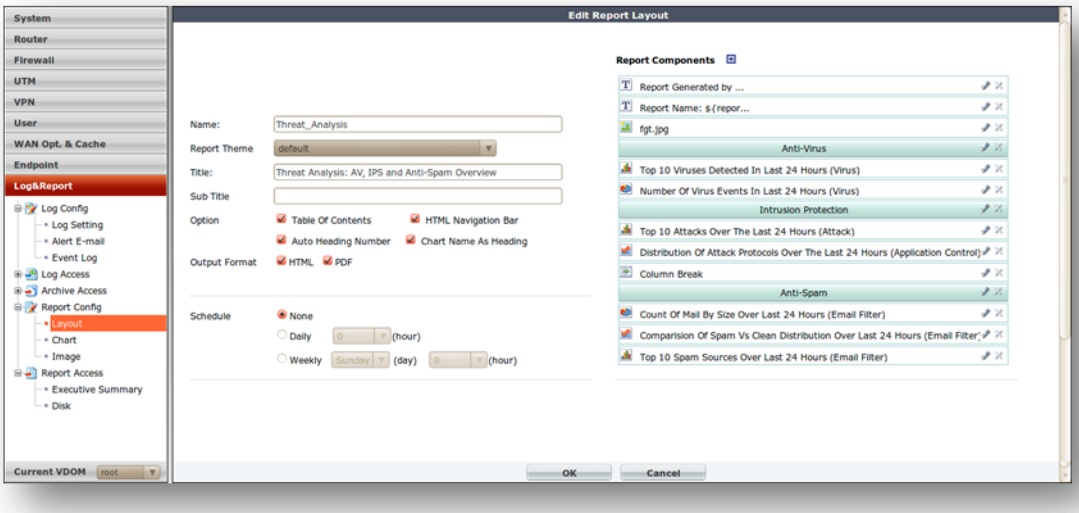
La base SQL intégrée au boitier offre une flexibilité sans pareil dans la création de rapport et la consultation de logs. A partir de la CLI, l'utilisateur peut créer une commande SQL et afficher le résultat dans un widget graphique ou un rapport complet téléchargeable. L'avantage de l'utilisation d'une requête SQL est de repousser les limites dans la personnalisation des rapports et d'améliorer la granularité des informations recueillies.

Exemple de widget graphique

Reporting

La partie reporting du fortiOS a beaucoup évolué avec la version 4. Le format SQL a introduit une nouvelle flexibilité dans la création des rapports mais aussi une meilleure correspondance avec le fortiAnalyzer.

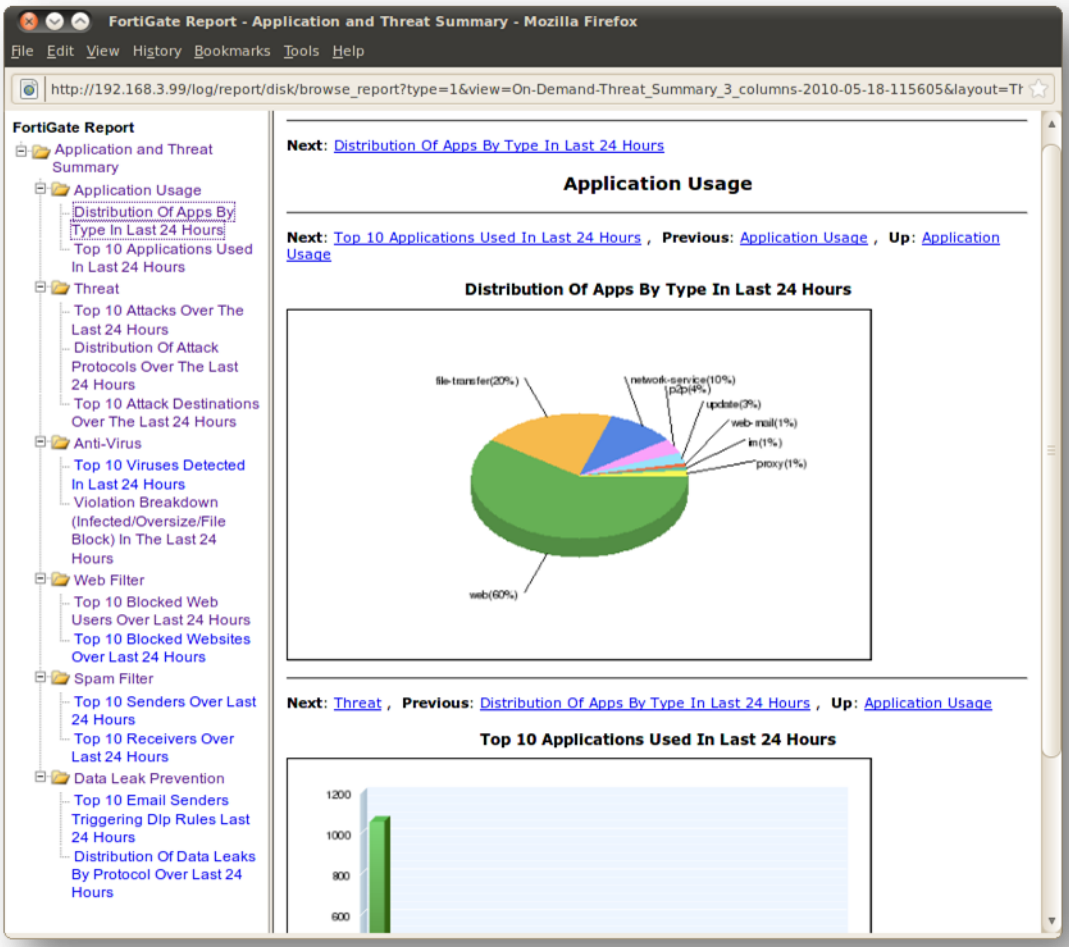
L'interface de création des rapports du fortiOS permet de personnaliser son document avec des logos, des titres, des graphiques modifiables (choix du type de graphique en histogrammes, camemberts ou courbes, choix des variables en abscisses et ordonnées), des filtres sur les directions du trafic ou des noms des utilisateurs. Le rapport s'architecture en paragraphes ou thèmes (VPN, filtrage web, antivirus…) au sein desquels l'utilisateur peut sélectionner les informations qu'il souhaite voir apparaître. Des informations ou « charts » sont proposées à l'utilisateur qui peut aussi les personnaliser ou en créer des nouveaux grâce à des requêtes SQL.



Interface de configuration du rapport

Les rapports obtenus sont téléchargeables (PDF, HTML) après une génération manuelle ou automatique par le système. Les rapports créés sur le fortiAnalyzer ou depuis la fortigate sont visibles sur le boitier FortiGate via la GUI.

Ainsi le FortiGate offre une véritable base de reporting et de journalisation des évènements intervenus sur le boitier. Les logs SQL du FortiAnalyzer peuvent aussi être exportés sur une base externe.



Exemple de rapport obtenu sur la Fortigate