



**Communiqué de Presse –**

**Contact Presse :**

Annabelle SOU  
Fortinet, Inc.  
+33 4 89 87 05 76  
[asou@fortinet.com](mailto:asou@fortinet.com)

**Fortinet Annonce de Nouvelles Fonctionnalités et un Nouveau Boitier de Pare-feu Applicatif Web**

*FortiWeb 4.0 MR3, Premier et Unique Pare-Feu Applicatif Web à Intégrer un Scanner des Vulnérabilités Web et des Fonctionnalités d'Optimisation des Performances au sein d'une Seule Appliance*

**Sophia Antipolis, 16 Août 2011-** Fortinet® (NASDAQ: FTNT) - l'un des principaux acteurs du marché de la sécurité réseau et le leader mondial des systèmes unifiés de sécurité UTM (Unified Threat Management) – annonce aujourd'hui une nouvelle version majeure de sa gamme de pare-feux applicatifs Web (WAF) FortiWeb™, pour les entreprises, fournisseurs de services applicatifs, de SaaS et de services d'infogérance en sécurité (MSSP). Les nouvelles appliances de pare-feux applicatifs Web de Fortinet sont les premiers et seuls systèmes de l'industrie à intégrer un scanner des vulnérabilités Web et des fonctions avancées d'équilibrage des charges dans un seul dispositif visant à réduire considérablement les temps de déploiement et l'utilisation des ressources tout en améliorant les performances des applications.

En plus des mises à jour logicielles, Fortinet a également lancé l'appliance FortiWeb-3000CFsx, qui offre désormais aux grandes entreprises, aux fournisseurs de services applicatifs et de cloud, des performances plus élevées au travers de son port fibre en mode « fail open ».

Grâce à l'intégration d'un scanner de vulnérabilités Web et d'un WAF, FortiWeb 4.0 MR3 est idéal pour les organisations soumises à l'exigence 6.6 de la norme PCI (Payment Card Industry

Data Security Standards), aux exigences relatives aux notifications d'intrusions telles que les réglementations California State Assembly Bill 1386 ou HIPAA. Pour les clients qui ont besoin d'aide en matière de protection d'applications Web contre les attaques telles que les injections SQL et Cross-Site Scripting, les appliances FortiWeb tirent profit du scanner des vulnérabilités Web intégré pour identifier de manière proactive et se prémunir contre la perte de données potentielle en se basant sur le Top 10 des failles de sécurité OWASP (Open Web Application Security Program). En outre, FortiWeb 4.0 MR3 dispose de fonctionnalités avancées en matière de compression des données pour améliorer l'utilisation de la bande passante et les temps de réponse, ainsi que la performance globale des applications.

### **Les nouvelles fonctionnalités FortiWeb 4.0 MR3**

FortiWeb 4.0 MR3 dispose d'une large gamme de nouvelles fonctionnalités facile qui couvre la sécurité et la configuration, les logs et les reporting ainsi que la simplicité d'utilisation :

- Un nouveau schéma de protection des dénis de service (DoS) offre des règles DoS pour les couches applicatives et réseau. Cela permet aux appliances FortiWeb d'analyser les requêtes provenant d'utilisateurs et de déterminer si elles sont authentiques ou si elles cachent des attaques automatisées.
- Une nouvelle fonction de Période de Blocage (*Period Blocking*) améliore la protection de l'organisation en permettant aux administrateurs de bloquer les utilisateurs pour des périodes déterminées plutôt que de refuser l'accès sur la base d'une connexion particulière
- La compression avancée a également été ajoutée pour permettre une utilisation plus efficace de la bande passante et un meilleur temps de réponse en compressant la récupération des données depuis les serveurs
- Les nouvelles améliorations de l'équilibre des charges permettent des contrôles de routine basés sur le contenu et proposent des alertes supplémentaires en cas de panne du serveur. L'authentification Radius/LDAP est également supportée pour plus de protection lors d'une connexion aux appareils FortiWeb. De plus, l'accès aux mises à jour FortiGuard – délivrant les informations de dernières minutes sur les menaces,

vulnérabilités et recherches en matière de sécurité – sont téléchargeables via un proxy.

Pour des logging et reporting améliorés, FortiWeb intègre désormais FortiAnalyzer™ de Fortinet permettant d'offrir un moyen simplifié de gestion centralisée de tous les logs et rapports à partir de multiples appareils FortiWeb. En proposant une nouvelle interface analytique, les appliances FortiWeb sont désormais dotées d'outils pour aider les clients à comprendre l'usage des applications Web en utilisant différents critères tels que le nombre de demandes, les données transférées et les types d'attaques, tout en y indiquant leur situation géographique. Les nouvelles améliorations d'alertes sont également incluses, permettant aux administrateurs de sécurité de recevoir des notifications par emails et des alertes pour une variété de conditions telles que les faibles ressources du système, les problèmes de fonctionnement du serveur et les limitations en matière de sessions.

La gamme FortiWeb dispose également d'une interface utilisateur mise à jour et simplifiée qui est basée sur celle des appliances de sécurité consolidée FortiGate® de Fortinet. En conséquence, la configuration du système est extrêmement simplifiée et propose des fonctionnalités d'utilisation clés telles que la personnalisation des pages d'erreur.

*“Notre clientèle mondiale a clairement fait savoir que la protection des applications Web est une très haute priorité,”* déclare Michael Xie, fondateur, Directeur Technique et Vice-Président de l'Ingénierie chez Fortinet. *“En parallèle, étant donné les contraintes de ressources de sécurité et IT, nous comprenons parfaitement la nécessité de consolider les principales fonctionnalités dans une seule appliance multi-usages qui peut être gérée de manière unifiée pour une simplicité de déploiement, une protection des données optimale et une utilisation des ressources maximale. Le lancement de notre nouvelle gamme de produits FortiWeb souligne notre engagement à répondre aux demandes de nos clients mondiaux.”*

### **Disponibilité**

FortiWeb 4.0 MR3 et l'appliance FortiWeb-3000CFsx sont d'ores et déjà disponibles.

## A propos de Fortinet ([www.fortinet.com](http://www.fortinet.com))

Fortinet (code NASDAQ : FTNT) est un des principaux fournisseurs de solutions de sécurité réseau et le leader du marché des systèmes unifiés de sécurité **Unified Threat Management** ou UTM. Nos produits et services d'abonnements assurent une protection étendue, intégrée et efficace contre les menaces dynamiques, tout en simplifiant l'infrastructure de sécurité informatique. Parmi nos clients figurent des administrations, des fournisseurs d'accès et de nombreuses entreprises, dont la plupart font partie du classement 2009 du Fortune Global 100. FortiGate, le produit phare de Fortinet, intègre des processeurs ASIC pour une meilleure performance et plusieurs fonctions de sécurité conçues pour protéger les applications et les réseaux contre les menaces Internet. Au-delà de ses solutions UTM, Fortinet offre une large gamme de produits conçus pour protéger le périmètre étendu des entreprises – du terminal au périmètre et au cœur de réseau, en passant par les bases de données et applications. Fortinet, dont le siège social se trouve à Sunnyvale en Californie (États-Unis), dispose également de bureaux dans le monde entier.

###

*Copyright © 2011 Fortinet, Inc. Tous droits réservés. Les symboles ® et ™ indiquent respectivement les marques déposées et non enregistrées de Fortinet, Inc., et de ses filiales et partenaires. Les marques Fortinet incluent mais ne sont pas limitées : Fortinet, FortiGate, FortiGuard, FortiManager, FortiMail, FortiClient, FortiCare, FortiAnalyzer, FortiReporter, FortiOS, FortiASIC, FortiWiFi, FortiSwitch, FortiVoIP, FortiBIOS, FortiLog, FortiResponse, FortiCarrier, FortiScan, FortiDB and FortiWeb. L'ensemble des marques commerciales citées dans le présent communiqué sont la propriété de leurs détenteurs respectifs. Fortinet n'a pas vérifié de façon indépendante les déclarations ou les certificats ci-dessus attribués à des tiers et Fortinet n'a pas approuvé de telles déclarations. Le présent communiqué peut contenir des déclarations prévisionnelles impliquant des incertitudes et des hypothèses. Si les risques ou les incertitudes se concrétisent ou si les hypothèses se révèlent inexactes, les résultats peuvent différer sensiblement par rapport à ceux exprimés ou sous-entendus. Toutes les déclarations autres que celles des faits historiques sont des déclarations qui pourraient être considérées comme des déclarations prévisionnelles. Fortinet n'a aucune obligation de mettre à jour les déclarations prévisionnelles dans l'éventualité où les résultats réels diffèrent et n'en a pas l'intention.*

**FTNT-O**