



Communiqué de Presse -

Contact Presse:

Annabelle Sou

Fortinet, Inc.

04 89 87 05 76

asou@fortinet.com

FORTINET® SECURISE LES TERMINAUX EN ETENDANT L'UTM AUX APPAREILS A DISTANCE

La Nouvelle Solution FortiClient™ Est Dotée d'un Logiciel Tout-en-Un Offrant un Accès Sécurisé à Distance pour Répondre aux Exigences Réglementaires et de Conformité

Sophia Antipolis, 12 Juillet 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 le lancement de FortiClient, un agent logiciel pour terminaux qui permet aux organisations de mettre en place des pratiques commerciales nécessitant une connectivité d'accès à distance sécurisée pour ses employés mobiles, fournisseurs et partenaires. En tant que solution de sécurité d'accès à distance tout-en-un, FortiClient améliore la sécurité de l'entreprise, aide les organisations à répondre aux exigences réglementaires et juridiques, ainsi qu'à appliquer les politiques de conformité pour empêcher les appareils non-autorisés d'accéder au réseau d'entreprise.

FortiClient est important à la stratégie produit de Fortinet, offrant une solution de sécurité flexible et étendue, du périmètre au cœur du réseau, avec des services managés centralisés.

La conception ultra-modulaire de la solution FortiClient comprend des fonctions essentielles d'encryption de données, d'authentification, de contrôle d'accès des terminaux et d'optimisation WAN dans un seul et même agent endpoint, facile à utiliser et léger à supporter. Pour plus de flexibilité, les administrateurs de sécurité peuvent choisir parmi plusieurs méthodes d'implémentation pour sécuriser les privilèges d'accès à distance des différentes catégories d'utilisateurs. Cela offre aux organisations la liberté de soit exploiter toute la suite des fonctionnalités de l'agent, soit choisir des fonctions spécifiques basées sur des besoins individuels de connectivité d'accès à distance. Par exemple, les administrateurs de sécurité peuvent vouloir implémenter l'encryption du trafic IPsec pour les employés à temps plein et l'encryption SSL pour les fournisseurs et partenaires.

Fortinet a conçu FortiClient pour plus de flexibilité en termes de déploiement, et permet à un logiciel tiers de coexister sur les terminaux. Les clients n'ont pas à retirer leurs applications anti-malwares actuelles pour déployer FortiClient.

Simplifier la Sécurité des Terminaux

Fonctionnant conjointement avec les appliances de sécurité consolidées FortiGate® de Fortinet, le FortiClient se focalise sur quatre fonctionnalités clés, toutes à partir d'un seul agent, pour supporter les différents besoins de sécurité d'accès à distance de ses clients:

- **VPN IPsec et SSL pour l'encryption des données.** Un simple assistant de configuration est fourni pour créer des politiques VPN de client-à-site pour des accès à distance. Le SSL-VPN en mode tunnel et le *tunneling* partagé offrent la liberté de se connecter à distance en utilisant un accès Web.

- **Authentification à deux facteurs pour la vérification d'identité.** FortiClient supporte totalement Local, RADIUS, LDAP, SecurID (via le Proxy RADIUS), FortiToken, ainsi que les options d'authentification par email et SMS.
- **Le Contrôle des Terminaux** empêche les appareils non conformes d'accéder au réseau, permettant aux entreprises d'appliquer leurs politiques de sécurité au périmètre du réseau.
- **L'optimisation WAN** réduit la consommation de la bande passante, accélère les performances réseau, diminue le temps de téléchargement et améliore l'efficacité du HTTP, FTP, CIFS, MAPI et du trafic général TCP.

Fortinet est le seul acteur capable de consolider ce large éventail de fonctionnalités de sécurité d'accès à distance dans un seul et même agent logiciel, offrant aux clients des options de déploiement inégalées, selon les besoins, avec une licence tout compris. Pour rivaliser les fonctionnalités du FortiClient, les offres concurrentes nécessitent des appliances supplémentaires, de nouveaux accords de licences et/ou de nouvelles consoles de gestion. Et dans certains cas, les fournisseurs concurrents ne supportent pas les fonctionnalités spécifiques de sécurité des terminaux proposés par FortiClient.

“FortiClient est un élément vital de notre stratégie de sécurité de bout-en-bout pour les clients Grands Comptes et PME.” déclare Michael Xie, fondateur, Directeur Technique et Vice-Président de l'Ingénierie chez Fortinet. *“En consolidant un tel ensemble de fonctionnalités de sécurité dans un agent logiciel simple à déployer, tous nos clients, petits et grands, peuvent désormais mettre en place, à travers un système de sécurité unique, le bon type de connexion d'accès à distance en fonction du type d'utilisateur. Ainsi, les meilleures pratiques commerciales nécessitant un accès à distance sécurisé*

peuvent être facilement et rentablement implémentées, ce qui a pour effet de réduire le TCO de l'entreprise."

Fortinet annonce également le lancement de FortiManager 4.0MR3 et FortiAnalyzer 4.0MR3, une mise à jour du système d'exploitation qui apporte des améliorations en matière d'utilisation et de gestion du *workflow*, ainsi que le support amélioré pour IPv6. FortiManager fournit une gestion, configuration et mise à jour des règles centralisées pour les appliances FortiGate, FortiWiFi™ et FortiMail™. FortiAnalyzer offre des fonctions de gestion de sécurité avancées telles que l'archivage des dossiers en quarantaine, la corrélation des événements, les évaluations des vulnérabilités, l'analyse du trafic et l'archivage des emails, l'accès Web/Internet, la messagerie instantanée et le contenu des transferts de fichiers

Disponibilité

Le nouvel agent FortiClient ainsi que le FortiManager 4.0 MR3 et le FortiAnalyzer 4.0 MR3 sont désormais disponibles.

A propos de Fortinet (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