11 FONCTIONS INTÉRESSANTES DONT DEVRAIT DISPOSER VOTRE PARE-FEU

Allez au-delà du simple blocage des menaces réseau pour protéger, gérer et contrôler le trafic des applications

SONICWALL®

Table des matières

SONICWALL®

Le pare-feu évolue

Les pare-feu traditionnels à inspection des paquets dynamiques se chargent de bloquer les menaces de la couche réseau en évaluant les ports et les protocoles utilisés par le trafic de la couche réseau. Les derniers pare-feu de nouvelle génération (NGFW) utilisent une inspection approfondie des paquets pour scanner la charge totale des paquets afin de fournir une prévention avancée contre les intrusions, des anti-malware, un filtrage du contenu et un anti-spam. De nombreuses applications sont acheminées par les ports communs de partage Web et les protocoles HTTP ou HTTPS. Cela empêche effectivement les pare-feu traditionnels de voir ces applications et de hiérarchiser le trafic productif et sécurisé par rapport au trafic non productif et potentiellement dangereux. Les pare-feu de nouvelle génération fournissent des renseignements sur les applications elles-mêmes, chose essentielle pour les professionnels des réseaux.

Avec la prolifération de l'informatique dans le cloud et des technologies Web 2.0, les pare-feu doivent relever un nouveau défi : le contrôle des applications.

SONICWALL®

Que fait le service SonicWall Application Intelligence and Control ?

Les pare-feu SonicWall vous permettent d'identifier et de contrôler toutes les applications utilisées sur votre réseau. Ce contrôle supplémentaire améliore la conformité et la prévention des fuites de données en identifiant des applications basées sur leurs signatures uniques plutôt que sur des ports ou protocoles. Pour ce faire, il est nécessaire de visualiser le trafic des applications afin de déterminer les schémas d'utilisation et de créer des règles granulaires associées aux applications, aux utilisateurs, voire aux groupes d'utilisateurs, ainsi qu'à l'heure de la journée et autres variables, permettant un contrôle flexible répondant à toutes les exigences du réseau.

Affectez la bande passante aux applications critiques ou sensibles à la latence.

Comment fonctionne le service SonicWall Application Intelligence and Control ?

Grâce à une vaste bibliothèque de signatures, enrichie en permanence et automatiquement mise à jour, SonicWall identifie des applications en se basant sur leur « ADN », plutôt que sur des attributs moins spécifiques, tels que le port source, le port de destination ou le type de protocole. Vous pouvez, par exemple, autoriser la messagerie instantanée, mais bloquer le transfert de fichiers ou autoriser l'accès à Facebook, mais bloquer l'accès aux jeux proposés sur Facebook. Ces contrôles sont également disponibles pour tout le trafic chiffré TLS/SSL qui doit être inspecté au même titre que les connexions non chiffrées. Et vous pouvez visualiser facilement les résultats de vos contrôles, ce qui vous permet d'affiner l'utilisation des applications et d'optimiser la consommation de la bande passante du réseau.

Contrôlez des catégories d'applications, des applications individuelles, mais aussi certaines caractéristiques spécifiques à ces applications.

La visualisation des applications vous permet de « voir » les navigateurs utilisés avant de créer la règle.

1re fonction intéressante :

Contrôler les applications autorisées sur le réseau

Vous voulez vous assurer que tous vos employés utilisent la dernière version d'Internet Explorer. Votre mission consiste à vous assurer que tous les employés lançant IE9 ou IE10 sont automatiquement redirigés vers le site de téléchargement d'IE11 et que tout autre accès à Internet est restreint. Vous disposez des solutions suivantes :

- Vérifier physiquement la version du navigateur Web de chaque système, chaque jour
- Écrire un script personnalisé pour vérifier automatiquement les versions du navigateur
- Mettre en place une règle avec le service SonicWall Application Intelligence and Control, et arrêter de s'inquiéter

Créer une règle redirigeant les utilisateurs IE9 ou IE10 vers le téléchargement du dernier navigateur IE et bloquer l'accès à Internet par IE9 ou IE10

1. Le moteur d'inspection approfondie des paquets (DPI) recherche l'agent utilisateur = IE 9.0 ou l'agent utilisateur = IE 10.0 dans l'en-tête HTTP
2. La règle redirige les utilisateurs d'IE9 ou IE10 vers le site de téléchargement IE11, tout en bloquant l'accès par IE9 ou IE10 à d'autres pages Web

SONICWALL

2e fonction intéressante :

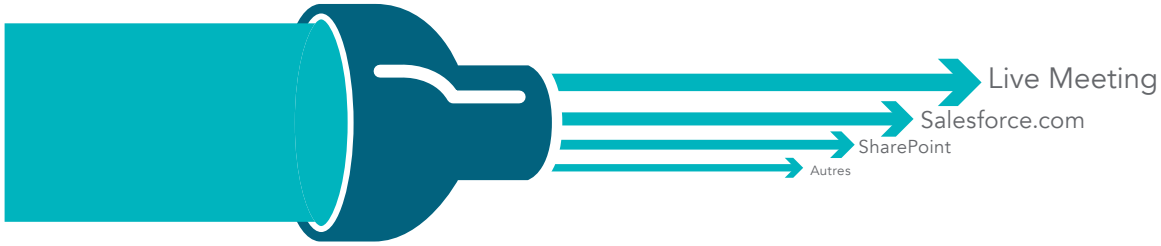
Gérer la bande passante pour des applications critiques

De nombreuses applications critiques, telles que Live Meeting, Salesforce.com® et SharePoint®, sont basées dans le cloud ou fonctionnent sur des réseaux géographiquement dispersés. Le fait de s'assurer que ces applications ont la priorité sur la navigation Web non productive améliore la productivité de l'entreprise.

Créer une règle accordant la priorité sur la bande passante à l'application Live Meeting

1. Le moteur d'inspection approfondie des paquets recherche la signature ou le nom de l'application
2. Attribuer à l'application Live Meeting une priorité supérieure sur la bande passante

La priorité des applications peut reposer sur la date (pensez à la priorité de fin de trimestre pour les applications de vente).



SONICWALL®

3e fonction intéressante :

Bloquer les applications P2P

Les applications pair à pair (P2P) non productives comme BitTorrent sont souvent utilisées pour télécharger des versions non autorisées de médias protégés par droits d'auteur, et peuvent rapidement saturer la bande passante ou transmettre des logiciels malveillants. Cependant, la création de nouvelles applications P2P, ou de simples modifications (par ex., des numéros de version) aux applications P2P existantes, se produisent en permanence, aussi il est difficile de bloquer manuellement une application P2P unique.

SonicWall met à jour en permanence la base de données d'Application Intelligence and Control en y ajoutant de nouvelles applications P2P dès qu'elles sont disponibles. Vous pouvez désormais créer une seule règle pour bloquer toutes les applications P2P.

Créer une règle pour bloquer l'utilisation des applications P2P

1. Le moteur d'inspection approfondie des paquets utilise des signatures prédéfinies d'application P2P à partir de la liste de signatures de l'application
2. Choisir les applications P2P dans la liste de signatures prédéfinies
3. Appliquer la règle à tous les utilisateurs
4. Bloquer les applications P2P par des restrictions de bande passante et d'horaires

Liste de signatures d'applications

BitTorrent-6.1
BitTorrent-6.0.3
BitTorrent-6.0.2
BitTorrent-6.0.1
... et des centaines d'autres

+

Liste de signatures d'applications

Les mises à jour de SonicWall sont reçues et appliquées

=

Liste de signatures d'applications

BitTorrent-6.1.1
BitTorrent-6.1
BitTorrent-6.0.3
BitTorrent-6.0.2
... et des centaines d'autres

The Results

- Vous pouvez gérer et contrôler les applications P2P
- Vous n'avez pas besoin de passer du temps à mettre à jour les règles des signatures IPS

SONICWALL

4e fonction intéressante :

Bloquer les composants non productifs des applications

Les applications de réseaux sociaux telles que Facebook, Instagram et YouTube sont devenues de nouveaux canaux de communication pour les particuliers comme pour les entreprises. Même s'il peut être contre-productif de bloquer toutes les applications de réseaux sociaux, vous souhaiterez peut-être contrôler la façon dont elles peuvent être utilisées sur le lieu de travail.

Vous pouvez ainsi laisser le personnel marketing mettre à jour la page Facebook de l'entreprise, tout en lui interdisant de jouer à des jeux Facebook comme Texas HoldEm Poker ou Candy Crush Saga. Application Intelligence and Control vous permet de créer une règle permettant l'accès à Facebook, tout en bloquant les jeux.

Créer une règle pour autoriser Facebook, mais bloquer les jeux Facebook

1. Sélectionner « tous » les utilisateurs
2. Sélectionner « jeux Facebook » comme catégorie
3. Créer une règle unique empêchant tous les utilisateurs d'accéder aux jeux proposés sur Facebook

Vous pouvez également autoriser la messagerie instantanée, mais bloquer les transferts de fichiers par messagerie instantanée.

5e fonction intéressante :

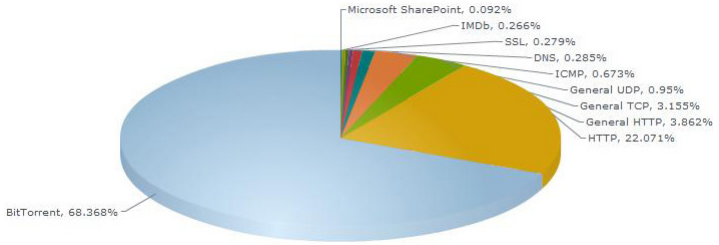
Visualiser le trafic de vos applications

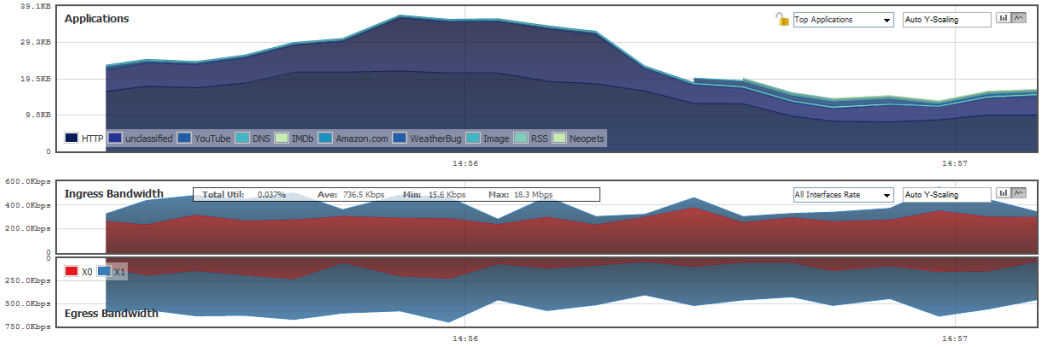
Que se passe-t-il sur mon réseau ? Qui gaspille ma bande passante ? Pourquoi mon réseau est-il si lent ? Vous êtes-vous déjà posé une de ces questions ? Vous pourriez utiliser une combinaison d'outils différents pour y répondre, mais cela prend du temps et ne vous fournira que des informations après coup. Grâce à la visualisation en temps réel du trafic des applications de SonicWall, vous pouvez répondre à ces questions instantanément, diagnostiquer rapidement les problèmes, détecter l'utilisation de réseaux non conformes, créer des règles appropriées et voir immédiatement l'efficacité de ces règles.

Afficher tout le trafic en temps réel en se connectant à l'Application Flow Monitor

1. Visualiser des graphiques en temps réel de tout le trafic des applications
2. Visualiser des graphiques en temps réel de la bande passante d'entrée et de sortie
3. Visualiser des graphiques en temps réel des sites Internet consultés et l'ensemble des activités des utilisateurs
4. Créer un filtrage personnalisé vous fournissant les informations les plus pertinentes

La visualisation donne aux administrateurs un retour instantané sur les flux du trafic réseau.





SONICWALL

6e fonction intéressante :

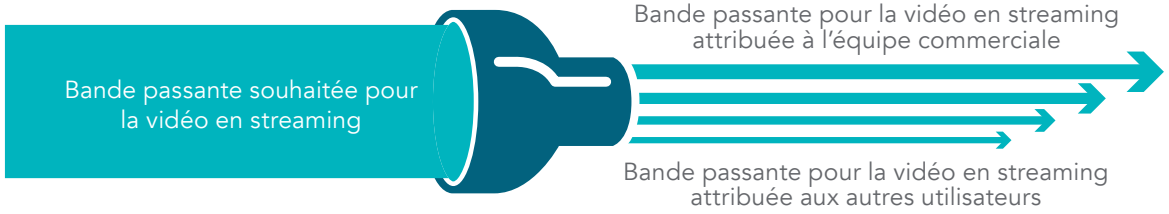
Gérer la bande passante pour un groupe d'utilisateurs

Que faites-vous si votre patron se plaint que les vidéos d'actualités qu'il veut regarder tous les matins sont instables et ne passent pas bien ? Après enquête, vous déterminez que cela est dû à une règle de gestion de la bande passante que vous avez mise en place à l'échelle de l'entreprise pour toutes les vidéos en streaming. Vous pourriez assouplir les restrictions de bande passante pour tout le monde, mais il existe désormais une meilleure solution : la gestion de la bande passante basée sur les groupes.

Créer une règle pour exclure l'équipe de direction de la gestion de la bande passante pour les vidéos en streaming

1. Choisir le groupe de direction importé depuis votre serveur LDAP
2. Le moteur d'inspection approfondie des paquets utilise des signatures d'application vidéo en streaming prédéfinies à partir de la liste de signatures de l'application
3. Appliquer une restriction de la bande passante sur le trafic comportant cet en-tête

Nombre d'entreprises ont trouvé que les employés sont plus heureux si vous leur laissez un accès complet à Internet, même si la bande passante est réduite pour les sites non productifs.



SONICWALL

7e fonction intéressante :

Bloquer les attaques de type ransomware et les infractions

La sécurité du réseau doit être au centre des préoccupations de tout administrateur informatique. La capacité à bloquer des attaques du type ransomware et des infractions véhiculées par les logiciels malveillants et les tentatives d'intrusion réduit considérablement les risques pour l'organisation et lui permet d'économiser des ressources qui auraient pu être gaspillées. Les services de sécurité de SonicWall, fonctionnant sur l'architecture hautes performances et à très faible latence des pare-feu de nouvelle génération SonicWall, sont capables de bloquer l'accès au réseau de millions de menaces connues et inconnues, avant qu'elles ne deviennent un danger pour votre organisation. SonicWall Capture élargit les capacités de prévention des menaces du pare-feu en détectant et en prévenant les attaques inconnues et « Zero Day » par le biais d'un service sandbox multimoteur basé sur le cloud.

Bloquez les attaques de logiciels malveillants et les intrusions avant qu'elles ne pénètrent dans votre réseau !

SONICWALL®

8e fonction intéressante :

Identifier les connexions par pays

Vous constatez une connexion à une adresse IP d'un pays étranger depuis votre bureau local voisin ou une succursale : s'agit-il d'une simple personne surfant sur Internet ou de l'activité d'un botnet ? Vous pouvez utiliser l'identification du trafic de pays GeoIP pour identifier et contrôler le trafic du réseau à destination ou provenant de pays spécifiques, soit pour vous protéger contre les attaques d'origines connues ou suspectées d'une activité de menace, soit pour enquêter sur le trafic suspect provenant du réseau.

Afficher les connexions par pays ou créer des filtres spécifiques à certains pays

1. Vérifier quelles applications se connectent aux IP d'autres pays
2. Voir quels utilisateurs et quels ordinateurs se connectent aux IP d'autres pays
3. Créer des filtres pour restreindre le trafic aux pays que vous spécifiez, avec des listes d'exclusion

Une fois que vous connaissez la réponse à la question, vous pouvez parler à l'utilisateur, inspecter la machine utilisant l'adresse IP incriminée ou activer un utilitaire de capture de paquets sur le pare-feu afin d'analyser exactement l'activité de cette connexion. En utilisant l'identification du trafic de pays GeoIP de SonicWall, vous pouvez identifier et résoudre des problèmes dont vous n'auriez peut-être pas eu conscience autrement.

9e fonction intéressante :

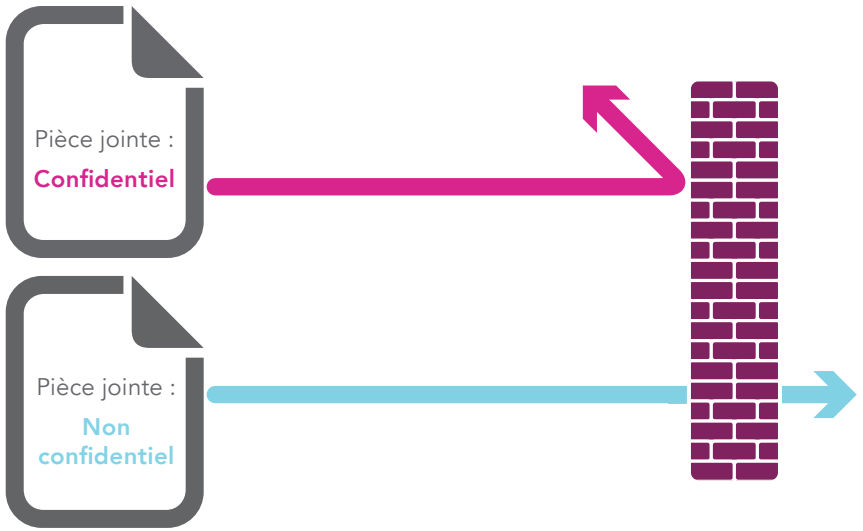
Empêcher les fuites de données par e-mail

Dans certaines sociétés, les e-mails sortants ne passent pas par leur système de sécurisation de la messagerie, ou ce système ne vérifie pas le contenu des pièces jointes. Dans les deux cas, les pièces jointes confidentielles peuvent facilement quitter l'organisation. Comme le trafic réseau sortant passe par votre pare-feu, vous pouvez détecter et bloquer ces « données en mouvement ».

Créer une règle pour bloquer les pièces jointes portant le tatouage numérique « Confidentiel »

Le moteur d'inspection approfondie des paquets recherche :

1. le contenu de l'e-mail = « Confidentiel » et
2. le contenu de l'e-mail = « Propriété de l'entreprise » et
3. le contenu de l'e-mail = « propriété privée », etc.



SONICWALL

10e fonction intéressante :

Empêcher les fuites de données sur la messagerie Web

Supposons maintenant que votre protection anti-spam existante puisse détecter et bloquer un e-mail sortant normal contenant des informations confidentielles. Et si un employé utilise une messagerie Web, comme Yahoo® ou Gmail®, pour envoyer des informations confidentielles ?

Créer une règle pour bloquer les pièces jointes confidentielles dans le trafic web

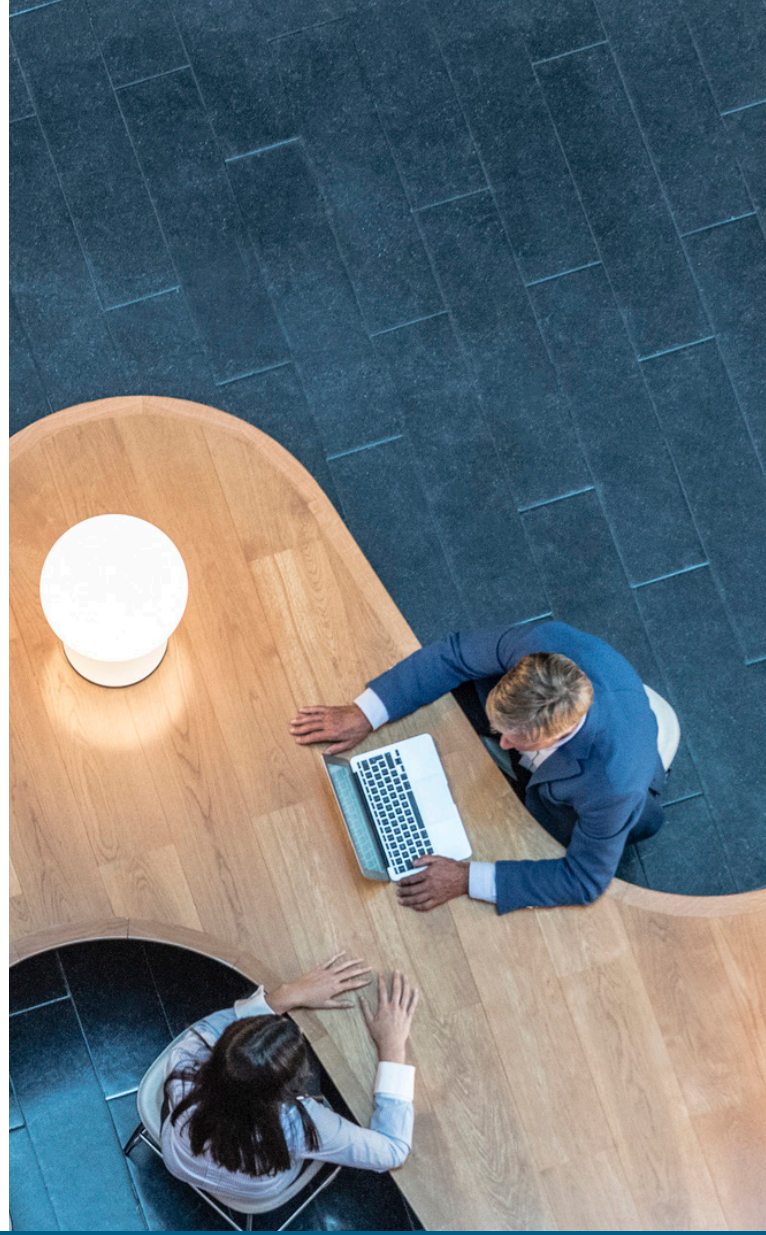
1. Le moteur d'inspection approfondie des paquets recherche « confidentiel » dans les fichiers transférés via http ou https
2. Bloquer le message et prévenir l'expéditeur que le message est confidentiel

OUI

De : le_bon@votre_entreprise.com
À : le_bon@partenaire.com
Objet : Validation de la carte de pointage - Jules
Je valide tes heures pour cette semaine. Jean

STOP

De : le_truand@votre_entreprise.com
À : le_truand@concurrent.com
Objet : Feuille de route de la conception
Voici la feuille de route.
9 janvier – Version 7.0
Ce document est **confidentiel**



Vous pouvez faire de même avec le contenu FTP.

11e fonction intéressante :

Gérer la bande passante pour le streaming audio et vidéo

L'accès à la vidéo en streaming depuis des sites comme YouTube.com est parfois utile, mais on observe souvent des abus. Le blocage de ces sites peut constituer une solution, mais il est préférable de limiter la bande passante totale accordée au streaming vidéo, quelle que soit la provenance. Cela s'applique également aux sites de streaming audio tels que les stations de radio en ligne et les services de musique en streaming tels que Spotify et Apple Music. Ce trafic ne doit pas nécessairement provenir de sites bien connus, mais peut aussi être hébergé sur des blogs. L'objectif est donc d'identifier ce trafic par ce qu'il est, plutôt que par son origine. L'inspection approfondie des paquets excelle dans cette activité.

Créer une règle pour limiter le streaming audio et vidéo par une liste de signatures prédéfinies

1. Sélectionner le streaming vidéo et audio dans les catégories d'applications
2. Déterminer la proportion de la bande passante que vous souhaitez affecter à ces catégories d'applications (par ex., 10 %)
3. Créer une règle imposant à tout le monde une consommation maximum de 10 % de la bande passante pour le streaming vidéo et audio (à l'exception éventuellement de certains groupes, comme le groupe de formation).
4. Le cas échéant, programmer la règle pour qu'elle s'applique pendant les heures normales de bureau, mais pas à l'heure du déjeuner ou après 18 h.
5. Confirmer l'efficacité de votre nouvelle règle par une visualisation en temps réel en vous connectant à l'Application Flow Monitor

SONICWALL®

Lorsque vous additionnez le tout

Plateforme hautes performances
+ Inspection approfondie des paquets
+ Prévention contre les intrusions
+ Veille, contrôle et visualisation des applications

Pare-feu de nouvelle génération SonicWall

Sécurité, performances et contrôle

SONICWALL®

Qui sommes-nous ?

Depuis plus de 27 ans, SonicWall lutte contre la cybercriminalité pour défendre les petites et moyennes entreprises dans le monde entier. Notre combinaison de produits et de partenaires nous permet d'offrir une solution automatisée de détection et de prévention des intrusions en temps réel adaptée aux besoins particuliers de plus de 500 000 organisations dans plus de 215 pays et territoires, pour vous permettre de développer vos affaires sans crainte. Pour en savoir plus, rendez-vous sur www.sonicwall.com ou suivez-nous sur Twitter, LinkedIn, Facebook et Instagram.

Si vous avez la moindre question concernant votre utilisation potentielle du présent contenu, merci de contacter :

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Veuillez consulter notre site Web pour obtenir des informations complémentaires.
www.sonicwall.com

Ebook-11CoolThings-Firewall-US-VG-MKTG5084

SONICWALL