



SonicWALL Comprehensive Anti-Spam Service

GESTION UNIFIÉE DES MENACES

Protection anti-spam instantanée au niveau de la passerelle

Quand on sait que le taux de courrier classé indésirable (spam, phishing, virus) atteint les 94 %, négliger ce trafic perturbateur et dangereux peut paralyser les communications commerciales et freiner la productivité de l'entreprise. L'élimination de ces pourriels dès la passerelle optimise le rendement du réseau et améliore la productivité, tant du personnel que de la messagerie électronique.

SonicWALL® Comprehensive Anti-Spam Service (CASS) s'installe en un instant sur les pare-feu SonicWALL pour offrir aux PME une protection exhaustive contre spam et virus. Par la réunion de plusieurs solutions et la fourniture en un clic de services anti-spam, CASS accélère le déploiement, simplifie l'administration et réduit les frais généraux. Sa configuration avancée ne prend que 10 minutes. CASS englobe l'ensemble des tâches associées au courrier entrant : anti-spam, anti-phishing, anti-malware, système de réputation IP du réseau SonicWALL GRID, gestion avancée des contenus, prévention des attaques par déni de service, quarantaine totale et résumés du courrier indésirable personnalisables au niveau utilisateur. Plus performant que le filtrage RBL, CASS offre une efficacité supérieure à 98 % contre le spam : plus de 80 % des spams sont bloqués au niveau de la passerelle, tandis que des techniques anti-spam évoluées telles que le filtrage Adversarial Bayesian™ analysent le reste du courrier.

Caractéristiques et avantages

Gestion avancée des réputations (ARM). Ce service se base sur la réputation des adresses IP émettrices pour rejeter le courrier indésirable (spam, phishing, virus en pièces jointes...) au niveau de la connexion, avant qu'il n'atteigne le réseau. Le réseau GRID de SonicWALL fournit des scores de réputation en temps réel qui permettent d'identifier et de bloquer le courrier suspect. La gestion avancée des réputations remplace les listes noires en temps réel, moins efficaces, lentes à répondre et sujettes à l'erreur.

Gestion avancée des contenus en nuage (ACM). Elimine tout courrier indésirable restant à l'aide des techniques SonicWALL éprouvées de lutte contre le spam : analyse « Adversarial Bayesian », empreintes GRID, moteur d'inférence graphique (IIE), détection de messages inintelligibles et analyse bayésienne du phishing. La conception en nuage exploite ces techniques anti-spam sophistiquées sans entraver le traitement du pare-feu ni le débit général du réseau.

Routage flexible du courrier indésirable. Classe les messages indésirables selon les catégories spam, spam probable, phishing, phishing probable, virus et virus probable. Les messages de chaque catégorie peuvent être rejetés, étiquetés et transmis, envoyés à la boîte de courrier indésirable de l'utilisateur ou détruits, garantissant ainsi un contrôle adéquat et le respect des contraintes de conformité de l'entreprise ou réglementaires.

Boîte de courrier indésirable utilisateur. Cette option permet de configurer rapidement des boîtes de courrier indésirable à la disposition des utilisateurs. Chaque utilisateur reçoit alors des résumés du courrier indésirable qui lui permettent de visualiser (en texte) les messages concernés et, s'il le souhaite, de les accepter. Le service informatique conserve le contrôle des catégories affichées, de la programmation et des délais de conservation des résumés de courrier indésirable.

GRID Anti-Virus. Cet antivirus est automatiquement activé avec SonicWALL CASS pour détecter les e-mails SMTP infectés et les réacheminer de la manière dont l'a défini l'administrateur (par ex. les rejeter ou les détruire) au niveau de la passerelle. S'ils sont achetés séparément, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service et SonicWALL Enforced Client Anti-Virus and Anti-Spyware Service fournissent une protection antivirus multicouche complète.

Listes d'autorisation et de blocage intégrées. Ces listes font partie intégrante des appliances de sécurité réseau SonicWALL. Les adresses IP peuvent être autorisées ou bloquées au niveau de la passerelle. La configuration des autorisations et blocages en fonction de personnes, de sociétés ou de listes permet un contrôle ciblé. Cette fonctionnalité est entièrement prise en charge par CASS et ne requiert aucune installation ni formation supplémentaire.

Reporting et journalisation intégrés. Ces services font également partie intégrante des appliances de sécurité réseau SonicWALL. Ils permettent de visualiser l'état et les statistiques de service par simple clic, et de consulter les entrées des fichiers journaux selon le nom du service. L'état de service affiche la disponibilité de Comprehensive Anti-Spam Service, des boîtes de courrier indésirable et du serveur de messagerie en aval.

Intégration LDAP flexible. Le service assure une gestion solide, simple et sécurisée des utilisateurs, avec un supplément de flexibilité grâce à la possibilité d'intégrer plusieurs LDAP.

Prise en charge des systèmes de sécurisation de messagerie en aval : règles de gouvernance d'entreprise ou de conformité, règles et préférences par utilisateur, service de reporting sophistiqué et autres, selon les besoins.

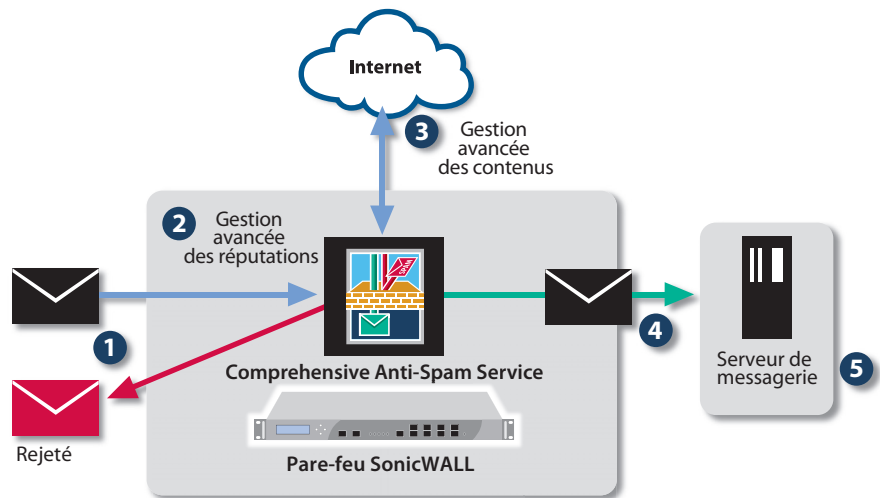
- Gestion avancée des réputations (ARM)
- Gestion avancée des contenus en nuage (ACM)
- Routage flexible du courrier indésirable
- Boîte de courrier indésirable utilisateur
- GRID Anti-Virus
- Listes d'autorisation et de blocage intégrées
- Reporting et journalisation intégrés
- Intégration LDAP flexible
- Prise en charge des systèmes de sécurisation de messagerie en aval

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Spécifications

Fonctionnement de SonicWALL Comprehensive Anti-Spam Service



- 1 Le trafic SMTP arrive sur le pare-feu SonicWALL.
- 2 Comprehensive Anti-Spam Service contrôle en temps réel la réputation du serveur IP émetteur sur la base du service de gestion avancée des réputations (ARM). L'ARM reçoit les données en temps réel de plus de 4 millions de postes de travail de par le monde, qui permettent de déterminer la réputation des serveurs émetteurs de courrier électronique. Près de 80 % du courrier indésirable peuvent être rejetés au niveau de la connexion, réduisant ainsi la charge de traitement du pare-feu.
- 3 Le courrier restant est traité par le service de gestion avancée des contenus en nuage (ACM) qui applique les techniques SonicWALL éprouvées de détection des spams.
- 4 Le courrier légitime parvient sur le serveur de messagerie.
- 5 En option, il est possible de parquer le courrier indésirable dans les boîtes SonicWALL prévues à cet effet sur le serveur de messagerie et d'envoyer par e-mail des résumés de courrier indésirable à chaque utilisateur.

Champ d'application de SonicWALL Comprehensive Anti-Spam Service

Les petites structures souhaitant rentabiliser le pare-feu SonicWALL dans lequel elles ont investi peuvent, grâce à CASS, garantir que seul le courrier légitime atteint leur serveur de messagerie. Les administrateurs gèrent CASS sur une seule et même interface intégrée au pare-feu. Les grandes entreprises peuvent ajouter une couche de protection anti-spam en plaçant CASS devant une solution SonicWALL Email Security, ce qui permettra de rejeter plus de 80 % du courrier indésirable au niveau de la connexion, et donc de réduire la charge de traitement de l'infrastructure en aval. Les entreprises distribuées, qui reçoivent du courrier sur différents sites, peuvent implémenter CASS sur les pare-feu SonicWALL distants en vue de réduire le trafic réseau indésirable et utiliser SonicWALL Email Security pour centraliser les services de protection de messagerie.

Plates-formes et serveurs de messagerie pris en charge

SonicWALL Comprehensive Anti-Spam Service est disponible en abonnement sur les produits SonicWALL suivants :

- séries TZ 100, TZ 200 et TZ 210 équipées de SonicOS 5.6.3 ou plus,
- toutes les appliances de sécurité réseau SonicWALL NSA et NSA E-Class équipées de SonicOS 5.6.3 ou plus,
- les plates-formes et/ou versions de SonicOS non mentionnées ne sont pas prises en charge.

SonicWALL Comprehensive Anti-Spam Service fonctionne avec tout serveur de messagerie acceptant les messages SMTP entrants.

Options offertes par Comprehensive Anti-Spam Service

L'option de **boîte de courrier indésirable utilisateur** requiert l'installation de l'application « Junk Store » (fait partie du service) sur un serveur (normalement le serveur de messagerie) équipé de Windows Server 2003 ou Windows Server 2008.



Comprehensive Anti-Spam Service

Comprehensive Anti-Spam Service pour TZ série 100 (1 an)
01-SSC-8985

Comprehensive Anti-Spam Service pour TZ série 200 (1 an)
01-SSC-8988

Comprehensive Anti-Spam Service pour TZ série 210 (1 an)
01-SSC-8991

Comprehensive Anti-Spam Service pour NSA 240 (1 an)
01-SSC-8994

Comprehensive Anti-Spam Service pour NSA série 2400 (1 an)
01-SSC-8997

Comprehensive Anti-Spam Service pour NSA 3500 (1 an)
01-SSC-9000

Références pluriannuelles disponibles. Veuillez consulter www.sonicwall.com.

Comprehensive Anti-Spam Service prend en charge un nombre illimité d'utilisateurs, mais est recommandé pour 250 utilisateurs ou moins.

La gamme complète de solutions de sécurité dynamique SonicWALL



SÉCURITÉ RÉSEAU



ACCÈS DISTANT SÉCURISÉ



SÉCURISATION WEB ET DE MESSAGERIE



SAUVEGARDE ET RÉCUPÉRATION



GESTION ET RÉGLES

SONICWALL

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™