Comprehensive Anti-Spam Service

Protection antispam instantanée au niveau de la passerelle

Quand on sait que le taux de courrier indésirable (spam, phishing, virus) atteint les 80 %, 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.

Le service CASS (Comprehensive Anti-Spam Service SonicWall®) s'installe en un instant sur les pare-feux SonicWall pour offrir aux PME une protection complète contre le spam et les 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. Le service CASS englobe l'ensemble des tâches associées au courrier entrant : protection et fonctionnalités antispam, anti-phishing, anti-malware, système de réputation IP du réseau SonicWall Capture Threat Network, 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, le service CASS offre une efficacité supérieure à 99 % contre le spam : plus de 80 % des spams sont bloqués au niveau de la passerelle, tandis que des techniques antispam évoluées telles que le filtrage Adversarial Bayesian™ et l'apprentissage machine analysent le reste du courrier.

Caractéristiques et avantages

Bloquez les attaques de spam, phishing et virus grâce aux nombreuses techniques éprouvées et brevetées*, notamment les contrôles de réputation qui vérifient non seulement la réputation de l'IP de l'expéditeur du message, mais aussi la réputation de son contenu, de sa structure, de ses liens, de ses images et de ses pièces jointes. Des techniques avancées sont également utilisées pour analyser le contenu des e-mails, comme le filtrage Adversarial Bayesian, l'analyse graphique et la détection de messages inintelligibles pour démasquer les menaces connues dissimulées et les nouvelles menaces. La conception Cloud exploite ces techniques antispam sophistiquées sans entraver le traitement du pare-feu ni le débit général du réseau.

Information sur les menaces en temps réel provenant du réseau Capture Threat SonicWall. Le réseau Capture Threat collecte et analyse les informations provenant des listes de menaces par secteur. Chaque jour, il examine et évalue rigoureusement des millions d'e-mails, établit des scores de réputation pour les expéditeurs et les contenus, et identifie les nouvelles menaces en temps réel pour offrir la protection la plus précise et la plus récente contre les nouvelles attaques de spam, tout en veillant à ce que le courrier légitime parvienne à destination.

SonicWall Capture Cloud. Le service exploite la technologie du réseau SonicWall Capture Threat Network pour assurer la protection antivirus et anti-logiciels espions basée sur le Cloud.

Routage flexible du courrier indésirable. Classifie les messages indésirables selon les catégories spam, spam probable, phishing, phishing probable, virus et virus probable. Ceux-ci 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

Avantages :

- Blocage des spams
- Protection contre les menaces en temps réel via le réseau SonicWall Capture Threat Network
- Capture Cloud
- Boîte de courrier indésirable utilisateur
- Listes d'autorisation et de blocage intégrées
- Reporting et journalisation intégrés
- Intégration LDAP
- Prise en charge des systèmes de sécurisation de messagerie en aval

** Brevets (États-Unis) : 7 814 545 ; 7 343 624 ; 7 665 140 ; 7 653 698 ; 7 546 348*

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.

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 aux administrateurs informatiques de définir un contrôle ciblé. Cette fonctionnalité est entièrement prise en charge par le service CASS et ne requiert aucune installation ni formation supplémentaire.

Fonctionnalités de reporting et de journalisation intégrées aux pare-feux SonicWall. Elles 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 du service CASS, 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 l'intégration LDAP.

Prise en charge des systèmes de sécurisation de messagerie en aval. Le service peut offrir des fonctionnalités telles que des stratégies de gouvernance ou de conformité de l'entreprise, des règles et des préférences par utilisateur, un service de reporting sophistiqué, ainsi que d'autres fonctionnalités selon les besoins.

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 au service CASS, garantir que seul le courrier légitime atteint leur serveur de messagerie. Les administrateurs gèrent le service CASS sur une seule et même interface intégrée au pare-feu. Les grandes entreprises peuvent ajouter une couche de protection antispam en plaçant le service 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 le service CASS sur les pare-feux SonicWall distants en vue de réduire le trafic réseau indésirable et utiliser SonicWall Email Security pour centraliser les services de protection de messagerie.

Plateformes et serveurs de messagerie pris en charge

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

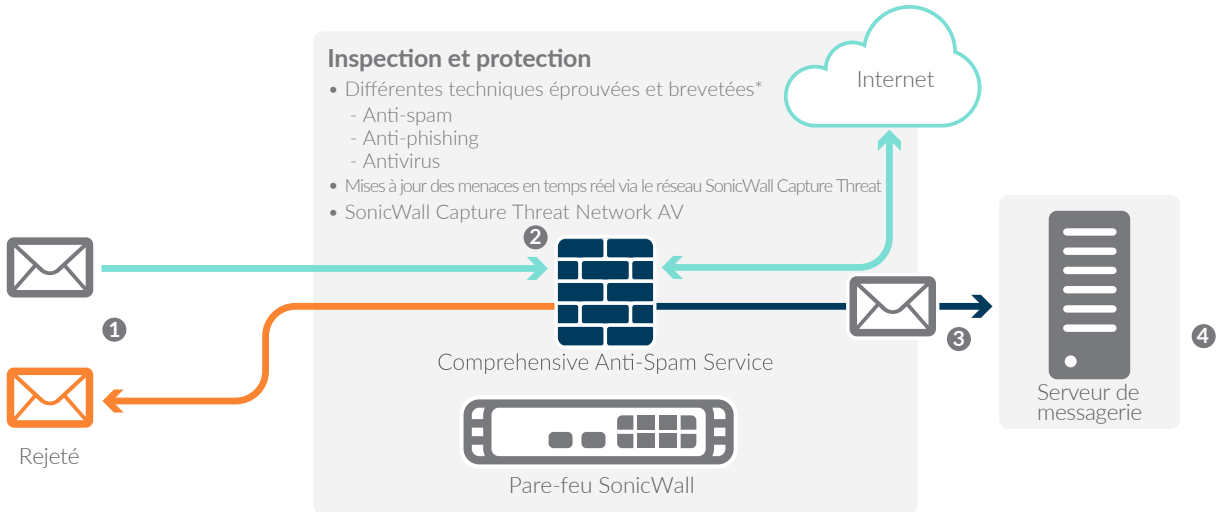
- tous les pare-feux SonicWall TZ Series et NS*a* (Network Security appliance)* équipés de SonicOS 5.6.3 ou versions ultérieures
- les plateformes et/ou versions de SonicOS non mentionnées ne sont pas prises en charge.

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 » (incluse dans le service) sur un serveur (normalement le serveur de messagerie) équipé de Windows Server 2008 ou de Windows Server 2012.

Fonctionnement de SonicWall Comprehensive Anti-Spam Service



1 Le trafic SMTP parvient au pare-feu SonicWall.

2 Comprehensive Anti-Spam Service contrôle en temps réel la réputation du serveur IP émetteur en temps réel. Le réseau SonicWall Capture Threat Network 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 peut être rejeté au niveau de la connexion, réduisant ainsi la charge de traitement du pare-feu. Le courrier restant est traité sur le Cloud par le réseau SonicWall Capture Threat Network qui applique les techniques SonicWall éprouvées de détection des spams.

3 Le courrier légitime parvient sur le serveur de messagerie.

4 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.

Comprehensive Anti-Spam Service

01-SSC-0682 SOHO Series (1 an)

01-SSC-0632 TZ300 Series (1 an)

01-SSC-0561 TZ400 Series (1 an)

01-SSC-0482 TZ500 Series (1 an)

01-SSC-0252 TZ600 Series (1 an)

01-SSC-2001 NS*a* 2650 (1 an)

01-SSC-4030 NS*a* 3650 (1 an)

01-SSC-4062 NS*a* 4650 (1 an)

01-SSC-4068 NS*a* 5650 (1 an)

01-SSC-9131 NS*a* 6600 (1 an)

** Sauf NSa 9250-9650*

Références pluriannuelles disponibles. Rendez-vous sur www.sonicwall.com.

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

À propos de nous

SonicWall s'engage depuis plus de 27 ans dans la lutte contre la cybercriminalité, défendant PME et grands comptes dans le monde entier. Notre alliance de produits et de partenaires nous a permis de mettre sur pied une solution automatisée de détection et de prévention des failles en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 215 pays et territoires, leur permettant de se concentrer sans crainte sur leur cœur de métier.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consultez notre site Internet pour plus d'informations.
www.sonicwall.com

DataSheet-CompAntiSpamService-US-VG-MKTG4092