



- **Gestion des menaces entrantes et sortantes**
- **Matériel, logiciel ou appliance virtuelle**
- **Architecture en mode réparti hautement disponible et évolutive**
- **Cadre de conformité réglementaire**
- **Gestion des règles de messagerie**
- **Gestion avancée de la réputation**
- **Parfaite intégration multi-LDAP**
- **Puissante fonction de reporting**
- **SonicWALL GRID Anti-Virus™**
- **Protection contre les attaques DHA, DoS et zombies**
- **Contrôle avancé par les utilisateurs finaux**
- **Rapidité d'installation et facilité de gestion**

Performances et évolutivité haut de gamme pour la sécurité du courrier électronique

Volumes croissants d'attaques sophistiquées par courrier électronique, exigence de conformité à des normes toujours plus strictes, dynamisme des environnements d'entreprise : nombre de fournisseurs de solutions de sécurisation de messagerie ne sont plus en mesure de relever les défis d'aujourd'hui. Les entreprises ont besoin de solutions puissantes, capables de limiter les coûts et la complexité de la sécurité.

Affichant un rapport prix/performance hors pair et la plus grande flexibilité du marché en matière de sécurisation de messagerie, la solution SonicWALL® E-Class Email Security fournit une protection extrêmement efficace et réactive, qui rationalise les coûts administratifs. Disponible sous forme d'appliance ESA, dont les modèles ES6000 et ES8300, de logiciel sur un serveur Windows® tiers ou d'appliance virtuelle dans un environnement VMware®, SonicWALL E-Class Email Security est une solution évolutive, dotée de fonctionnalités d'exécution et de mise à jour automatiques. L'analyse des trafics entrant et sortant lui permet de stopper les spams, virus ou attaques de phishing, mais aussi d'empêcher la fuite de données confidentielles, dopant ainsi d'une part la productivité et garantissant, d'autre part, le respect de la conformité réglementaire.

SonicWALL E-Class, c'est un ensemble de solutions professionnelles haut de gamme qui se distinguent non seulement par l'excellence des performances et de la protection offertes, mais aussi par leur évolutivité, leur grande simplicité et un rapport qualité/prix inégalé. La gamme de produits et services E-Class réunit un éventail complet de solutions de protection de messagerie, de sécurité réseau et d'accès distant sécurisé.

Caractéristiques et avantages

La **gestion des menaces entrantes et sortantes** filtre le courrier entrant afin de bloquer spams, phishing et autres malwares avant qu'ils n'infiltrer le réseau. Les e-mails et pièces jointes sortants sont également inspectés afin d'empêcher la fuite de données et la prolifération de malwares.

Il existe plusieurs options de déploiement flexibles : comme **matériel** (sur un boîtier hautes performances renforcé), comme **logiciel** serveur (au sein de l'infrastructure existante) ou comme **appliance virtuelle** (dans le cas de ressources informatiques partagées pour en optimiser l'utilisation, faciliter la migration et réduire les coûts).

Grâce à l'**architecture en mode réparti, hautement disponible et évolutive**, les entreprises sont libres de combiner les appliances matérielles et virtuelles et le logiciel SonicWALL E-Class comme elles le souhaitent, tout en les gérant de manière centralisée, contrairement aux limites imposées par les éditeurs concurrents. SonicWALL offre une solution de protection du courrier électronique réellement évolutive et hautement disponible pour l'archivage, l'externalisation, les services gérés, les fusions et acquisitions, ainsi que pour la mise en œuvre d'environnements distribués dans le monde entier.

Le **cadre de conformité réglementaire** permet aux entreprises d'identifier, de surveiller et d'établir de manière intelligente des rapports sur les messages ne respectant pas les règles et directives de conformité (HIPAA, SOX, GLBA, PCI). Il utilise le routage à base de règles pour envoyer les messages aux systèmes d'archivage et de chiffrement.*

La **gestion des règles de messagerie** permet d'appliquer diverses règles propres à l'entreprise, consistant notamment à stopper la propagation de contenus inappropriés, protéger les informations confidentielles, ajouter des avis de non-responsabilité au courrier ou bloquer la distribution de fichiers exécutables.

La **gestion avancée de la réputation** permet de rejeter jusqu'à 90 % des courriers indésirables connus au stade de la connexion, le reste étant éliminé au moment du filtrage avancé de SonicWALL Advanced Content Management. D'où une évolutivité et des performances optimisées, ainsi qu'une visibilité totale (contrairement aux produits d'autres marques).

La **parfaite intégration multi-LDAP** garantit une synchronisation automatique des solutions SonicWALL

E-Class Email Security avec différents serveurs LDAP, automatisant la gestion des adresses électroniques, des comptes et des groupes d'utilisateurs.

La **puissante fonction de reporting** permet l'établissement de rapports précis et personnalisables pour l'ensemble du système, qui renseignent notamment sur les types d'attaques, l'efficacité de la solution ou les performances du système. Dans le cas de déploiements en mode réparti, la surveillance et le reporting de tous les systèmes sont entièrement centralisés, ce qui permet d'économiser du temps et simplifie la gestion globale du système.

SonicWALL GRID Anti-Virus™ fournit une protection antivirus et anti-spyware basée sur la technologie SonicWALL. A cela s'ajoute l'abonnement aux mises à jour des signatures McAfee™ et Kaspersky Lab™ qui offre une couche supplémentaire de protection.

La **protection contre les attaques DHA, DoS et zombies***, ce sont d'abord de puissantes fonctions de gestion des connexions conçues pour suspendre, étouffer ou bloquer toute connexion douteuse avant qu'elle n'atteigne le système. En association avec les fonctions d'anti-spam, d'anti-phishing et d'antivirus SonicWALL, elles constituent une solution complète, venant à bout de tous les types d'attaques électroniques.

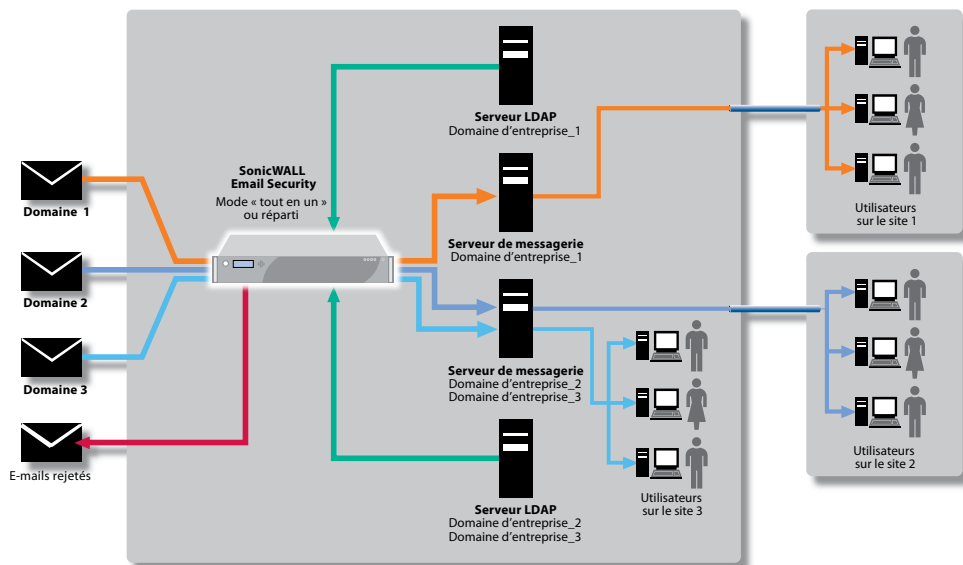
Le **contrôle avancé par les utilisateurs finaux** permet à ces derniers d'exercer un plus grand contrôle sur leur propre gestion des spams, les listes d'autorisation et de blocage, la sévérité de l'anti-spam et la délégation de comptes. Grâce au bouton « Courrier indésirable » pour Outlook®, dont il suffit de télécharger le plug-in, les utilisateurs finaux peuvent réagir activement face aux courriers indésirables qui parviennent jusqu'à leur boîte de réception. L'administrateur définit tous les contrôles cédés aux utilisateurs finaux et peut les attribuer en fonction d'un utilisateur, d'un groupe ou d'une fonction.

La **rapidité d'installation et la facilité de gestion** réduisent sensiblement le temps nécessaire à l'implémentation et à la gestion d'une solution complète de sécurisation de messagerie. La fonction Judgment Details facilite le débogage et évite aux messages légitimes de se retrouver dans le courrier indésirable.

* Ce service nécessite un abonnement supplémentaire.

Déploiements SonicWALL Email Security

L'architecture ultra-flexible de SonicWALL Email Security (SES) répond aux besoins des entreprises à la recherche d'une solution de protection de messagerie hautement évolutive, redondante et distribuée, gérable de manière centralisée. Les solutions SES peuvent être déployées en mode « tout en un » ou réparti. En mode réparti, les systèmes peuvent faire office d'analyseurs distants ou de centres de contrôle. Une installation typique en mode réparti comporte un ou plusieurs **analyseurs distants** connecté(s) à un **centre de contrôle** : l'**analyseur distant** reçoit les e-mails d'un ou de plusieurs domaines et applique les techniques correspondantes de gestion des connexions, de filtrage (anti-spam, anti-phishing et antivirus) et de règles avancées, avant de transmettre les messages inoffensifs au serveur de messagerie situé en aval. Le **centre de contrôle** gère de manière centralisée tous les analyseurs distants, collecte et stocke les courriers indésirables qui en proviennent. La gestion centralisée assume le reporting et la surveillance de tous les systèmes reliés. Reposant sur ce principe, la solution SonicWALL Email Security s'adapte pour assurer la protection du courrier entrant et sortant pour tous les types d'entreprises, de manière exhaustive et économique. Les appliances virtuelles SonicWALL Email Security permettent un déploiement total en mode réparti sur un ou plusieurs serveurs, optimisant ainsi les économies d'échelle.



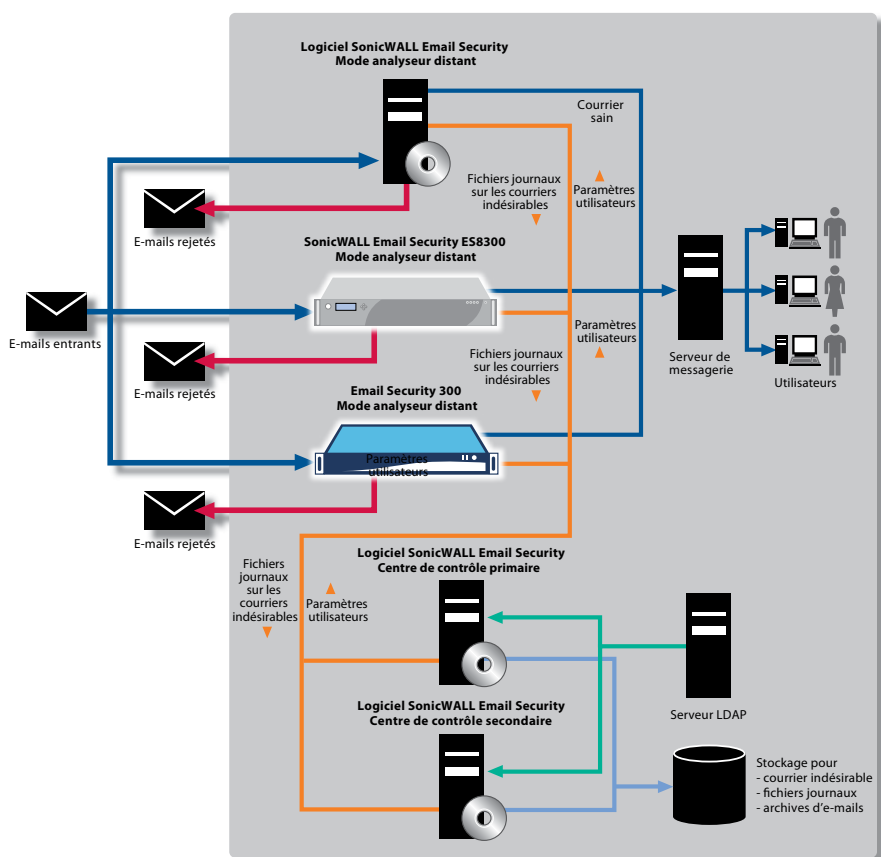
Domaines multiples, contrôle centralisé

Email Security centralise la gestion de plusieurs domaines de messagerie.

Utilisations typiques : groupes médicaux, compagnies d'assurance, franchises et entreprises multimarques/multidivisionnelles

Avantages

- Gestion centralisée et conviviale de plusieurs domaines
- Application des règles internes de messagerie (centralisées) à tous les employés et/ou en fonction des domaines/ groupes/utilisateurs
- Reporting centralisé par domaine
- Contrôle centralisé des courriers sortants pour appliquer les règles et les principes de routage par domaine ou à l'échelle de l'entreprise



Evolutivité et redondance

Très évolutif, ce système de sécurisation de messagerie avec gestion centralisée peut utiliser différents types de plates-formes (logiciel, appliance matérielle ou virtuelle) et intègre des fonctions de basculement automatique dans l'architecture comme dans le matériel.

Utilisations typiques : moyennes et grandes entreprises, structures qui présentent des exigences de disponibilité élevées concernant la sécurisation de messagerie, environnements à plates-formes mixtes ou entreprises pratiquant le stockage du courrier électronique sur un SAN (Storage Area Network)

Avantages

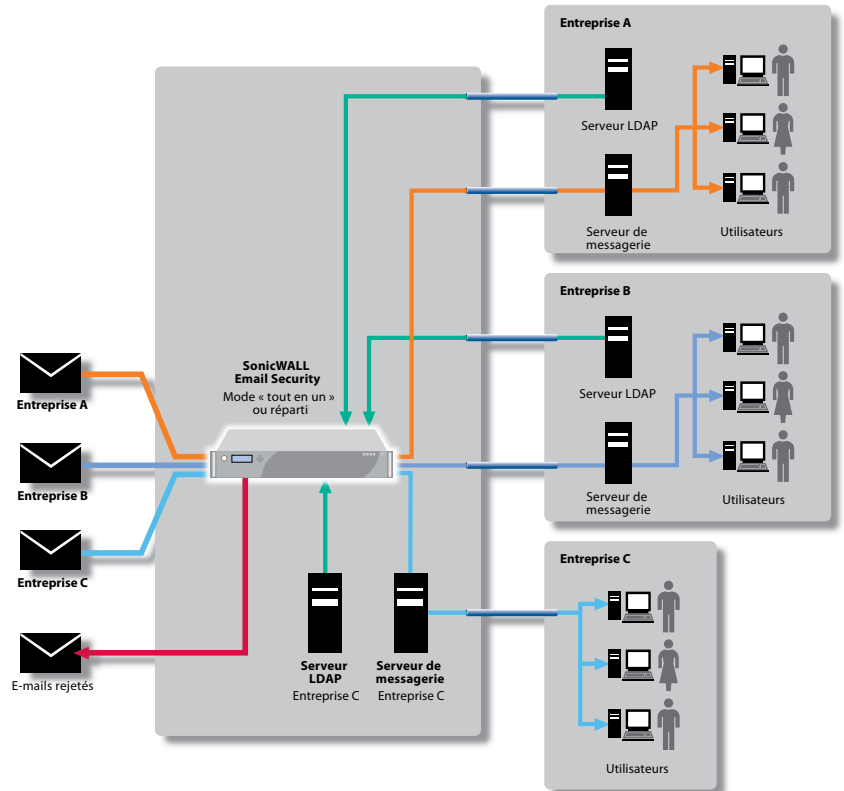
- Chaque analyseur distant peut basculer vers n'importe quel autre analyseur distant, ce qui garantit la continuité du flux de courrier électronique
- La présence de centres de contrôle primaires et secondaires garantit une redondance totale
- Le stockage des e-mails et autres contenus sur le SAN de l'entreprise permet de centraliser les données et simplifie les procédures de sauvegarde
- Le contrôle centralisé de plates-formes mixtes réduit les coûts de gestion
- L'ajout d'un analyseur distant est un moyen simple d'agrandir le système ou d'étendre le déploiement à d'autres sites, selon les besoins

Fournisseurs de services gérés

Les fournisseurs de services gérés (MSP) peuvent proposer à leurs clients des services de filtrage des e-mails, parfois également de serveur de messagerie. La solution SonicWALL Email Security est suffisamment flexible pour permettre aux MSP d'opérer une gestion centralisée de plusieurs domaines, tout en laissant aux clients la liberté de garder leurs propres utilisateurs, règles, boîtes de courrier indésirable et autres, le tout sous le contrôle du MSP.

Avantages

- Gestion centralisée de plusieurs domaines pour une suppression commune des courriers indésirables
- Règles de messagerie centralisées communes à tous et/ou règles propres à chaque client par domaine/groupe/utilisateur
- Reporting centralisé ainsi que par domaine
- Le contrôle centralisé sur le courrier sortant peut être utilisé pour certains ou tous les clients, et les règles/le routage peuvent être appliqués par domaine
- Les serveurs de messagerie et LDAP peuvent se trouver sur le site du client, sur le site du MSP, ou sur les deux à la fois
- Grâce à la flexibilité d'élargissement, le MSP peut démarrer avec un seul système, puis passer, selon ses besoins, à une architecture en mode réparti hautement évolutive, avec possibilités de basculement automatique
- Les appliances virtuelles accélèrent la mise en œuvre de la solution auprès de clients actuels ou nouveaux, tout en limitant les investissements supplémentaires ou les frais de déploiement



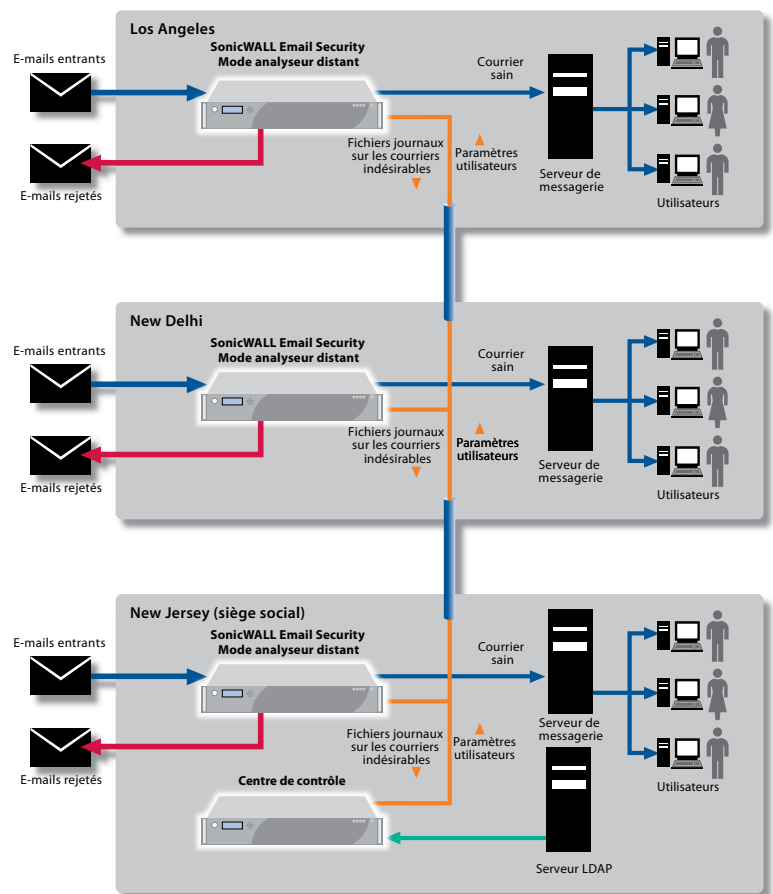
Des sites multiples, un contrôle centralisé

Pour les environnements distribués, il est difficile de définir l'emplacement optimal pour le traitement des e-mails : trop centralisé, il fait perdre un temps précieux au service informatique ; trop localisé, il peut compromettre la sécurité de l'entreprise. L'architecture flexible de SonicWALL Email Security propose une solution en parfaite adéquation avec les besoins spécifiques des entreprises distribuées.

Utilisations typiques : entreprises réparties sur plusieurs sites ou venant, par exemple, d'en acquérir de nouveaux, ou encore franchiseurs centralisant la gestion de messagerie pour leurs propres opérations ou celles des filiales franchisées

Avantages

- Traitement localisé des e-mails pour supprimer le courrier indésirable et transmettre les e-mails sains, ce qui réduit le trafic réseau
- Gestion centralisée de sites multiples, incluant l'application de règles, le reporting et la surveillance
- Contrôle centralisé du courrier sortant pour appliquer les règles et les principes de routage par domaine, par site ou à toute l'entreprise
- Clustering des analyseurs distants permettant le basculement automatique d'un site à un autre



Spécifications

SonicWALL E-Class Email Security



Appliances SonicWALL E-Class Email Security

SonicWALL Email Security ES6000
01-SSC-6604

SonicWALL Email Security ES8300
01-SSC-6609



Logiciel SonicWALL E-Class Email Security

SonicWALL Email Security Software
01-SSC-6636

Appliance virtuelle SonicWALL E-Class Email Security

SonicWALL Email Security
Virtual Appliance
01-SSC-7636

Abonnements – E-Class

Abonnements pack 5000 utilisateurs
SonicWALL Email Protection avec
support 24 x 7 (1 an)
01-SSC-6674

SonicWALL Email Compliance (1 an)
01-SSC-6644

Antivirus McAfee avec SonicWALL
Time Zero (1 an)
01-SSC-6764

Antivirus Kaspersky avec SonicWALL
Time Zero (1 an)
01-SSC-6774

(Pour obtenir les références d'autres
packs utilisateurs, consultez
www.sonicwall.com.)

Présentation des licences

SonicWALL E-Class Email Security (logiciel, appliance matérielle ou virtuelle)

- Agent MTA (Message Transfer Agent)
- Protection contre les attaques DHA (Directory Harvest Attack) et DoS (Denial of Service)
- Gestion Web
- Gestion des règles/filtrage des contenus d'e-mails
- Rapports et surveillance
- Synchronisation LDAP

Abonnement à Email Protection avec support dynamique (8x5 ou 24x7) – requis

- Anti-spam (1 an)
- Support 8x5 ou 24x7 (1 an)
- Anti-phishing (1 an)
- RMA (remplacement matériel)
- Mises à jour logiciel/firmware (1 an)

Service d'abonnement pour la conformité réglementaire

- Dictionnaires (fonctionnalité)
- Boîtes de validation
- Analyse des pièces jointes
- Filtrage des ID d'enregistrement
- Rapports de chiffrement
- Archivage d'e-mails
- Règles prédéfinies
- Rapports de conformité

Abonnement antivirus (Kaspersky Lab et/ou McAfee avec antivirus Time Zero SonicWALL)

- Antivirus Kaspersky
- Antivirus SonicWALL Time Zero
- Antivirus McAfee
- Détection de zombies

Appliances Email Security	PME (petits déploiements)		E-Class (grandes entreprises)	
	ESA 3300	ESA 4300	ES6000	ES8300
Nb de domaines	Illimité			
Système d'exploitation	Appliance avec SE Linux renforcé SonicWALL			
Châssis rackable	1RU		1U Mini	2U
Unité(s) centrale(s)	Intel 2,0 GHz	Intel Dual Core 2,0 GHz	3,2 GHz	Quad Core Xeon 2,0 GHz
Mémoire vive	2 Go	4 Go	2 Go	4 Go
Disque dur	250 Go	2 x 250 Go	2 x 160 Go	4 x 750 Go
Matrice de disques redondante (RAID)	–	RAID 1	X	RAID 5
Lecteurs remplaçables à chaud	–	–	–	X
Alimentation redondante	–	–	–	X
Dimensions	43,2 x 41,6 x 4,4 cm 17,0 x 16,4 x 1,7 in		42,7 x 35,6 x 4,3 cm 16,8 x 14,0 x 1,7 in	69,9 x 48,3 x 8,9 cm 27,5 x 19,0 x 3,5 in
Poids	7,26 kg 16 lbs		8,62 kg 19 lbs	22,7 kg 50 lbs
Poids DEEE	8,62 kg 16 lbs		6,35 kg 14 lbs	22,2 kg 48,9 lbs
Consommation (watts)	86	101	201	280
BTU	293	344	685,41	1098,0
MTBF à 25 °C en heures	125 004			
MTBF à 25 °C en années	14,27			

Logiciel Email Security	
Nb de domaines	Illimité
Système d'exploitation	Exécution sur Microsoft Windows 2003 Server ou Microsoft Windows 2008 Server
Unité centrale	Configuration minimum 2,66 GHz
Mémoire vive	Configuration recommandée 2 Go, configuration minimum 1 Go
Disque dur	Configuration minimum supplémentaire 40 Go
Appliance virtuelle Email Security	
Hyperviseur	ESXi™ et ESX™ (version 4.0 ou plus récente)
Système d'exploitation installé	SonicLinux renforcé
Mémoire allouée	2 Go
Taille du disque de l'appliance	80 Go
Guide de compatibilité matérielle VMware	http://www.vmware.com/resources/compatibility/search.php

Caractéristiques des appliances et logiciels : abonnements disponibles pour les grands déploiements en packs de 1 000, 2 000, 5 000 et 10 000 util.

Protection	
Protection e-mails entrants et sortants	Oui
Efficacité anti-spam	+98 %
Anti-phishing identifié séparément	Oui
SonicWALL GRID Anti-Virus	Oui
Antivirus : double couche commercial	Oui
Protection antivirus instantanée	Oui
Protection contre les attaques DHA, DoS, etc.	Oui
Accélérateur LDAP/Exchange	Oui
Prise en charge multi-LDAP	Oui
Gestion des connexions avec réputation d'IP	Oui
Service d'abonnement pour la conformité réglementaire	
Gestion puissante des règles	Oui
Analyse des pièces jointes	Oui
Dictionnaires	Oui
Boîtes de validation/flux de travaux	Oui
Installation et gestion	
Installation	< 1 heure
Gestion par semaine	< 10 min.
Compatibilité avec tous les serveurs de messagerie	Oui
Signature unique (SSO)	Oui
Gestion de groupes et d'utilisateurs	Oui
Configuration et mise en quarantaine par les utilisateurs finaux	Oui
Résumé du courrier indésirable avec option d'autorisation	Oui
Surveillance, reporting et gestion des journaux	Oui
Judgment Details	Oui
Moteur de recherche rapide de messages	Oui
Clustering et clustering à distance	Oui

La gamme SonicWALL de protection dynamique



SÉCURITÉ RÉSEAU



ACCÈS DISTANT SÉCURISÉ



SÉCURISATION WEB ET DE MESSAGERIE



SAUVEGARDE ET RÉCUPÉRATION



GESTION ET RÈGLES

SonicWALL France

T +33 1 49 33 73 19 France@sonicwall.com

SonicWALL BeNeLux

T +32 (0) 15 280 985 Benelux@sonicwall.com

Contacts du support SonicWALL

www.sonicwall.com/emea/4724.html

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™