DOSSIER TECHNIQUE : LA MIGRATION À PARTIR DE SMS FOR SMTP

symantec.
Confidence in a connected world.

Migrer de Symantec Mail Security for SMTP vers Symantec Brightmail Gateway

Livre blanc : instructions Symantec

Migrer de Symantec Mail Security for SMTP vers Symantec Brightmail Gateway

Sommaire

Introduction

Ce document détaille la migration à partir de Symantec Mail Security for SMTP (SMS for SMTP) vers Symantec Brightmail Gateway (SBG). Comme les messages affichés peuvent varier considérablement d'un environnement à l'autre, ce document ne propose pas de procédure de migration pas à pas mais présente le processus de migration de façon générale et propose des trucs et astuces permettant de faciliter la migration de SMS for SMTP vers SBG.

À propos de la migration de SMS for SMTP vers SBG

La migration de SMS for SMTP vers SBG est un processus principalement manuel. Le processus de migration compte trois tâches principales :

1. l'installation de SBG ;
2. l'enregistrement des paramètres clés de SMS for SMTP ;
3. la migration des paramètres de SMS for SMTP vers SBG.

Ce document se concentre sur les étapes deux et trois de ce processus. Pour obtenir des informations sur la première étape, veuillez consulter le *guide de démarrage* et le *guide d'installation* de SBG.

Planification de la migration

Avant de lancer la migration, les clients doivent disposer de la dernière version de SBG exécutée sur leur matériel 8300 Series ou sur leur plate-forme VMware. Des détails sur la dernière version et sur son téléchargement sont disponibles sur le site Web suivant :

http://www.symantec.com/business/support/overview.jsp?pid=53991

Lors de la planification du déploiement de SBG, assurez-vous de bien évaluer vos ressources matérielles conformément aux besoins de votre environnement. SBG peut être déployé sur les dispositifs 8300 Series ou sur le matériel de votre choix exécutant VMware ESX ou ESXi version 3.5. La configuration requise exacte peut différer de celle de SMS for SMTP, étant données les améliorations de traitement et de gestion des connexions apportées à SBG.

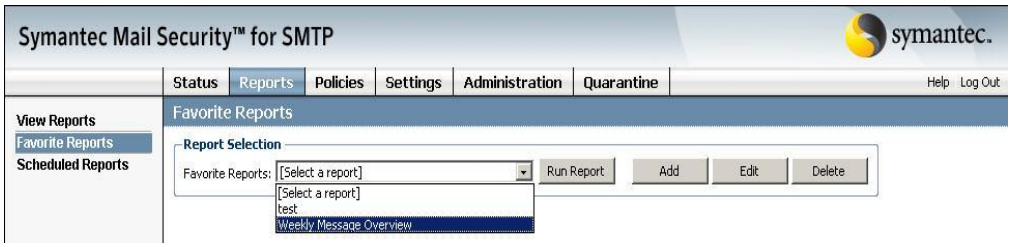
Pour un déploiement sur VMware, assurez-vous de respecter la configuration requise de Brightmail Gateway Virtual Edition.

Consultez le chapitre « Configuration requise et recommandations pour le déploiement virtuel » du guide de démarrage de SBG pour en savoir plus.

Enregistrement des paramètres clés de SMS for SMTP et migration vers SBG

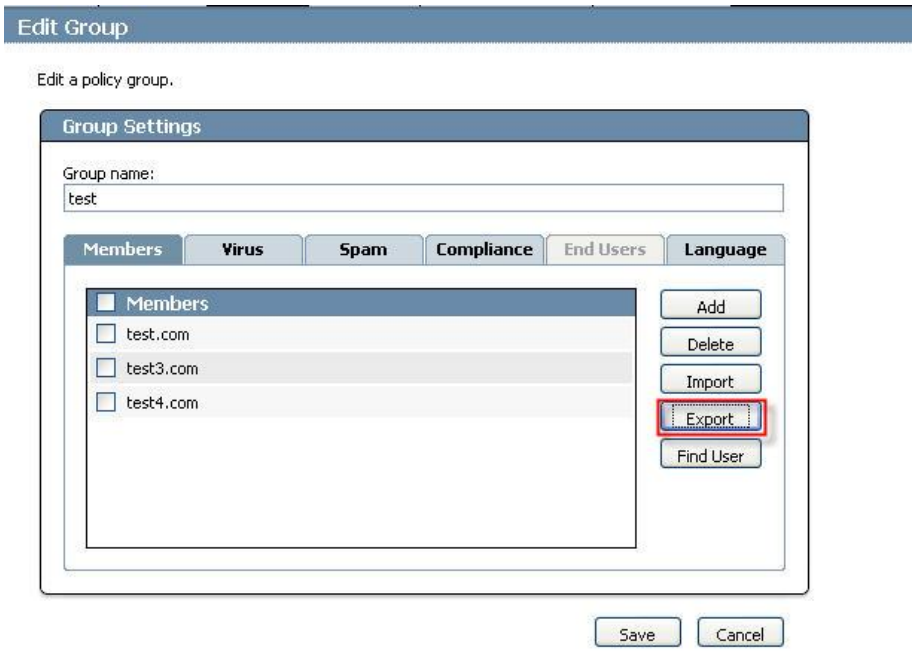
La liste ci-dessous répertorie les fonctionnalités et paramètres principaux que vous pourrez enregistrer afin de les intégrer à votre nouvel environnement SBG.

1. Rapports – Sur la page Reports (Rapports) de SMS for SMTP, cliquez sur les liens Favorite Reports (Rapports favoris) et Scheduled Reports (Rapports planifiés). Éditez les rapports de votre choix à partir de ces emplacements et consignez les détails de leurs paramètres afin de les dupliquer sous SBG. Lors de la création de ces rapports sous SBG, vous remarquerez peut-être que certains des rapports de SMS for SMTP ne sont plus proposés. Ils ont dans ce cas été remplacés par des outils de rapports plus puissants disponibles sous SBG.



2. Politiques de groupe – Listez toutes les politiques de groupe existantes dans l'environnement à partir de la page Policies (Politiques) -> Group Policies (Politiques de groupe). Pour chaque politique de groupe, consignez les informations suivantes :

    - les membres appartenant au groupe. Si l'adhésion au groupe n'est pas basée sur les groupes LDAP, ces données peuvent être exportées dans un fichier texte afin d'être ensuite importées sous SBG comme le montre l'image ci-dessous. Si l'adhésion au groupe est basée sur les groupes LDAP, ces informations sont déjà enregistrées et les groupes pourront être ajoutés au nouveau groupe sous SBG après la configuration de la synchronisation de la source LDAP.



    - Consignez aussi les détails des politiques de virus en incluant le nom des différentes politiques appliquées à chaque type de verdict. Sur la page Policies (Politiques) -> Filter Policies (Politiques de filtre) -> Virus (Virus), éditez les différentes politiques appliquées au groupe et enregistrez les actions à entreprendre (dans la majorité des cas le nom de la politique donne certaines indications, comme l'action à entreprendre). Lors de la configuration de SBG, vous pourrez créer des politiques similaires à appliquer aux nouveaux groupes créés.
    - Consignez aussi les détails des politiques de spam en incluant le nom des différentes politiques appliquées à chaque type de verdict. Sur la page Policies (Politiques) -> Filter Policies (Politiques de filtre) -> Spam (Spam), éditez les différentes politiques appliquées à vos groupes et enregistrez les actions à entreprendre (dans la majorité des cas le nom de la politique donne certaines indications, comme l'action à entreprendre). Lors de la configuration de SBG, vous pourrez créer des politiques similaires à appliquer aux nouveaux groupes créés.

- Listez toutes les politiques de conformité appliquées aux groupes en incluant le nom des différentes politiques appliquées à chaque groupe. Sur la page Policies (Politiques) -> Filter Policies (Politiques de filtre) -> Conformité, éditez les différentes politiques de groupe et enregistrez les conditions et actions à entreprendre pour les différentes politiques. Lors de la création de ces groupes sous SBG, vous pourrez profiter des améliorations significatives apportées aux fonctionnalités de filtrage avancé des contenus et de prévention des pertes de données. Vous pourrez aussi étudier les moyens d'optimiser vos politiques grâce aux nouvelles fonctionnalités proposées.

3. Politiques de pare-feu de messagerie électronique – Sur la page Policies (Politiques) -> Email Firewall Policies (Politiques de pare-feu de messagerie électronique), listez toutes les politiques de pare-feu de messagerie électronique activées :

    - Des attaques sont-elles configurées sur la page Attacks (Attaques) ? Consignez si les attaques DHA sont activées. Le cas échéant, les attaques DHA peuvent être de nouveau activées une fois la synchronisation LDAP configurée sous SBG. Il existe aussi une nouvelle option privilégiée sous SBG permettant d'activer la fonctionnalité DHA avec une nouvelle source LDAP de validation des destinataires. Consultez le *Guide d'administration SBG* pour en savoir plus.
    - Si vous souhaitez activer la fonctionnalité Spam Attack (Attaque de spam), vous remarquerez qu'elle a été remplacée sous SBG par la nouvelle fonctionnalité Connection Classification (Classification des connexions), activée par défaut à l'installation de SBG. Consultez le *Guide d'administration SBG* pour en savoir plus.
    - Si vous souhaitez activer la fonctionnalité Virus Attack (Attaque de virus), enregistrez les seuils configurés et appliquez des paramètres similaires sur la page Reputation (Réputation) -> Senders (Expéditeurs) -> Email Virus Attacks (Attaques de virus par courrier électronique) de SBG.
    - Si l'authentification de l'expéditeur est activée, consignez la technologie d'authentification utilisée (SPF ou ID de l'expéditeur), les domaines pour lesquels elle est activée et les actions à entreprendre lorsque l'authentification d'un message échoue. Ces paramètres pourront être dupliqués sous SBG sur la page Spam (Spam) -> Settings (Paramètres) -> Sender Authentication settings (Paramètres d'authentification de l'expéditeur).
    - Sur la page Sender Groups (Groupes d'expéditeurs), consultez les éventuelles listes activées et renseignées d'expéditeurs bloqués ou autorisés (suivant le domaine, l'adresse IP ou les services tiers). Si rien n'est configuré, aucune action n'est requise. Si l'une de ces listes a été renseignée, consignez l'action à entreprendre pour chaque liste spécifiée. Éditez chacune de ces listes puis exportez les données qu'elles contiennent, via la fonctionnalité d'exportation, à un fichier intitulé « allowedblockedlist.txt ». Sous SBG les listes d'expéditeurs autorisés et bloqués ont été rebaptisées respectivement Good Senders (Expéditeurs bienveillants) et Bad Senders (Expéditeurs malveillants). Le fichier « allowedblockedlist.txt » peut être importé sous SBG à partir de toute liste d'expéditeurs locale sur les pages Reputation (Réputation) -> Policies (Politiques) -> Good and Bad Senders (Expéditeurs bienveillants et malveillants), via la fonctionnalité d'importation. Une fois la liste importée, assurez-vous de définir l'action requise pour les différentes listes et d'activer les listes de votre choix.
    - Les listes d'expéditeurs via proxy ouvert et celles de spammeurs suspectés ont été remplacées sous SBG par la liste Symantec Global Bad Senders (Liste mondiale Symantec des expéditeurs malveillants). Ces listes sont bien plus efficaces sous SBG, et Symantec recommande formellement de les activer et de conserver leurs actions de rejet par défaut.
    - La liste des expéditeurs sûrs a été remplacée sous SBG par la liste Symantec Global Good Senders (Liste mondiale Symantec des expéditeurs bienveillants). Symantec recommande formellement d'activer cette liste et de conserver ses actions de rejet par défaut.

4. Ressources des politiques – Sur la page Group Policies (Politiques de groupe) -> Policy Resources (Ressources des politiques), consignez les informations suivantes :

    - Si des annotations personnalisées ont été créées et sont utilisées par les politiques de conformité, consignez leurs noms et éditez-les afin de pouvoir copier et coller le texte dans un éditeur de texte. Vous pourrez ensuite créer de nouvelles annotations et y coller le texte correspondant sur la page Conformité -> Resources (Ressources) -> Annotations (Annotations) de SBG.
    - Si l'action d'archivage est utilisée par l'une de vos politiques, consignez l'adresse électronique d'archivage, l'hôte et le port du serveur puis saisissez ces données sur la page Conformité -> Settings (Paramètres) -> Archive de SBG.
    - Si des listes de pièces jointes personnalisées ont été créées, consignez leurs noms et éditez-les pour enregistrer l'ensemble des classifications de fichiers, extensions et MIME associés à la liste. Vous pourrez ensuite recréer ces listes sous SBG sur la page Conformité -> Resources (Ressources) -> Attachment Lists (Listes de pièces jointes). Vous remarquerez aussi que SBG dispose de listes de pièces jointes intégrées améliorées et plus complètes que SMS for SMTP.
    - Si des dictionnaires personnalisés ont été créés, consignez le nom du dictionnaire, éditez-le et sélectionnez tous les mots en faisant glisser la souris puis copiez et collez-les dans un éditeur de texte. Enregistrez-le en tant que fichier texte, puis recréez la liste sous SBG sur la page Conformité -> Resources (Ressources) -> Dictionaries (Dictionnaires). Vous pouvez ensuite utiliser la fonctionnalité d'importation de votre nouveau dictionnaire pour importer le fichier texte contenant les mots de votre ancien dictionnaire. Vous remarquerez aussi que SBG a considérablement étoffé les dictionnaires disponibles par défaut et que de nombreux dictionnaires ont été développés pour éviter la perte de données et améliorer la conformité.
    - Si des notifications personnalisées ont été créées, listez leurs noms puis éditez-les et consignez les informations sur l'expéditeur de la notification, son destinataire, l'objet, le corps du message et si le message original doit être inclus à la notification ou non. La notification peut ensuite être recrée sous SBG sur la page Conformité -> Resources (Ressources) -> Notifications (Notifications). Vous remarquerez que SBG propose d'ajouter des variables d'attribut aux messages afin de permettre une plus grande personnalisation des notifications. Consultez le *Guide d'administration SBG* pour en savoir plus.

5. Si vous avez configuré des paramètres de spam suspect, consignez la valeur seuil (comprise entre 25 et 89) puis saisissez cette même valeur sous SBG sur la page Spam (Spam) -> Settings (Paramètres) -> Scan Settings (Paramètres d'analyse). Assurez-vous que la politique de spam suspecté est activée sous SBG et configurée afin de correspondre à la configuration de la politique de SMS for SMTP.

6. Dans la rubrique Settings (Paramètres) -> Analyse du courrier électronique -> Virus (Virus), consignez la configuration de LiveUpdate. Saisissez la même configuration sous SBG sur la page Virus (Virus) -> Settings (Paramètres) -> LiveUpdate (LiveUpdate). SBG prend en charge la configuration de différentes sources pour le flux de mise à jour des définitions de l'antivirus : via le téléchargement direct des définitions de virus Platinum ou via un hôte LAN configuré ou un hôte proxy. Si vous avez configuré une exclusion d'un type de fichier pour l'analyse de virus sous SMS for SMTP, vous pouvez définir la même exclusion sous SBG sur la page Virus (Virus) -> Settings (Paramètres) -> Settings (Paramètres) -> Scan Settings (Paramètres d'analyse) -> Exclude Scanning (Exclure de l'analyse). De même, si vous avez configuré un niveau de précision du limier sous SMS for SMTP, vous pouvez définir le même niveau de précision sous SBG sur la page Virus (Virus) -> Settings (Paramètres) -> Scan Settings (Paramètres d'analyse) -> General (Général).

7. Si vous avez configuré des paramètres de conteneur (dans Settings (Paramètres) -> Analyse du courrier électronique -> Analyse) sous SMS for SMTP, les mêmes seuils peuvent être définis manuellement sous SBG sur la page Protocols (Protocoles) -> SMTP -> Settings (Paramètres) -> Scan Settings (Paramètres d'analyse).

8. Si vous disposez de serveurs LDAP définis pour l'authentification ou la synchronisation, vous devrez les ajouter sous SBG avec les mêmes informations administrateur et détails de requête sur la page Administration -> Settings (Paramètres) -> LDAP. Sélectionnez le serveur LDAP d'authentification et/ou synchronisation. Vous remarquerez que les sélections de routage, destinataire et validation sont nouvelles sous SBG. Veuillez consulter le *Guide d'administration SBG* pour en savoir plus.

9. Sur la page Settings (Paramètres) -> System Settings (Paramètres du système) de SMS for SMTP, si vous avez configuré des paramètres de quarantaine pour le spam et les virus suspectés, vous pourrez les dupliquer manuellement sous SBG sur la page Spam (Spam) -> Settings (Paramètres) -> Quarantine Settings (Paramètres de la quarantaine) pour la quarantaine du spam et Virus (Virus) -> Settings (Paramètres) -> Suspect Virus Settings (Paramètres des virus suspectés) pour la quarantaine des virus suspectés. Si vous avez configuré des paramètres de rapport (données des rapports et paramètres de suppression), ils pourront être reconfigurés sous SBG sur la page Administration -> Settings (Paramètres) -> Reports (Rapports) -> Report Settings (Paramètres des rapports). Si vous avez configuré des paramètres de journaux (niveau des journaux, limites de stockage de la base de données des journaux, suppression, journaux d'analyse et de suivi des messages et paramètres Syslog), ils pourront être configurés de la même façon sous SBG sur la page Administration -> Settings (Paramètres) -> Logs (Journaux). Vous remarquerez que l'onglet Distant autorise la génération de journaux à distance via Syslog. Veuillez consulter le *Guide d'administration SBG* pour en savoir plus.

10. Si vous avez configuré des fonctionnalités de brouillage des adresses et de création d'alias sous SMS for SMTP, copiez les entrées dans un fichier texte qui pourra ensuite être importé sous SBG sur les pages Administration -> SMTP -> Address Masquerading (Brouillage des adresses) et Aliases (Alias). Vous remarquerez que la fonctionnalité d'importation de SBG prend en charge les fichiers texte :

    - pour importer les entrées masquées, importez une liste des adresses masquées à partir d'un fichier similaire à la table « virtusertable » de Sendmail. Lorsque vous cliquez sur Import (Importer) à partir de la page de brouillage des adresses, la page Import Masqueraded Entry (Importation d'entrées masquées) s'affiche. Indiquez le fichier contenant les entrées masquées, puis cliquez sur Import (Importer). Une fois l'importation achevée, vous pourrez générer un rapport répertoriant les entrées non traitées. Remarque : les fichiers incluant des caractères ASCII étendus ou non ASCII ne peuvent pas être traités. Vous ne pouvez importer que des fichiers encodés au format US-ASCII.
    - Pour l'importation des alias, chaque adresse du fichier texte doit être séparée par un ou plusieurs espaces ou tabulations, ou une combinaison d'espaces et de tabulations. Les virgules et points-virgules ne sont pas des séparateurs valides. Dans le fichier à importer, chaque ligne doit contenir une adresse d'alias suivie d'une ou plusieurs adresses de destination.

11. Pour exporter la configuration des domaines locaux de votre installation SMS for SMTP, vous pouvez copier les domaines locaux existants dans un fichier texte et l'importer sous SBG sur la page Protocols (Protocoles) -> SMTP -> Domains (Domaines). Assurez-vous que la liste des définitions de domaines locaux et adresses électroniques applique le format US-ASCII dans un fichier similaire à la table « mailertable » de Sendmail. Vous pourrez inclure à la définition des informations facultatives de routage vers des hôtes de destination locaux par défaut.

12. Si vous avez configuré des administrateurs multiples et défini plusieurs rôles pour chacun, vous devrez rajouter manuellement les administrateurs et leurs adresses électroniques avec renforcement facultatif des mots de passe sous SBG sur la page Administration -> Users (Utilisateurs) -> Administrators (Administrateurs). Consignez la granularité des droits d'administration pour les dossiers de conformité, et si l'administrateur doit recevoir ou non les notifications des incidents. Notez aussi qu'il peut vous être demandé de réinitialiser les mots de passe administratifs par défaut de SBG pour les remplacer par ceux déjà configurés dans votre installation SMS for SMTP.

13. Si vous avez défini des alertes dans votre installation SMS for SMTP (dans Settings (Paramètres) -> System Settings (Paramètres du système) -> Alerts (Alertes)), consignez l'expéditeur des alertes et leurs conditions pour les redéfinir ensuite sous SBG sur la page Administration -> Settings (Paramètres) -> Alerts (Alertes). Vous remarquerez que les conditions d'alerte sont plus développées sous SBG, répondant à un plus grand nombre d'événements.

14. Si vous avez défini une « reverse address binding strategy (stratégie de liaison d'adresse inversée) » dans la configuration de votre SMS for SMTP (dans Settings (Paramètres) -> Hosts (Hôtes) -> [sélectionnez l'hôte] -> SMTP -> Advanced Settings (Paramètres avancés)), veuillez noter qu'il n'existe pas de fonction similaire sous SBG, car ses nouvelles fonctionnalités offrent une plus grande flexibilité permettant à l'administrateur de sélectionner les liaisons de livraison SMTP par interface. Cette fonctionnalité peut être configurée sur la page Administration -> Hosts (Hôtes) -> Configuration (Configuration) -> [sélectionnez l'hôte] -> SMTP -> Advanced Settings (Paramètres avancés) -> SMTP Delivery Bindings (Liaisons de livraison SMTP).

Quels sont les éléments exclus de la migration ?

Bien qu'il soit possible de recréer la majeure partie de la configuration de SMS for SMTP sous SBG, la plupart des données sauvegardées dans le Control Center de SMS for SMTP ne pourront pas être exportées vers le Control Center de SBG. Elles comprennent les statistiques en cours et les données de rapports, de quarantaine et de journaux.

Si les utilisateurs finaux ont accès à leur quarantaine de spam personnelle et disposent des droits nécessaires pour créer leurs propres listes d'éléments autorisés et bloqués et pour définir les paramètres de langue utilisés pour l'authentification et de la synchronisation LDAP, ces paramètres ne seront pas conservés. Les utilisateurs finaux peuvent copier et coller ces paramètres dans un fichier texte afin de recréer leurs listes dans la quarantaine de SBG.

A propos de Symantec
Symantec est le leader mondial de solutions de gestion de la sécurité, du stockage et des systèmes, pour aider les entreprises et les particuliers à sécuriser et à administrer leurs informations. Basée à Cupertino (Californie), Symantec est présente dans plus de 10 pays. Des informations supplémentaires sont disponibles à l'adresse www.symantec.fr

Pour connaître les coordonnées des bureaux dans un pays spécifique, visitez notre site Web. Pour obtenir des renseignements sur les produits aux Etats-Unis, veuillez appeler le 1 (800) 745 6054

Symantec Corporation
Symantec (France) SAS
Tour Egée, 17 avenue de l'Arche
92671 Courbevoie Cedex
01 41 45 02 02

www.symantec.fr