

Axway MailGate

Protégez votre réseau de messagerie de l'extérieur et de l'intérieur



Alors que le volume des messages parvenant au réseau de votre entreprise croît, la menace d'intrusions indésirables et potentiellement malveillantes se renforce. En parallèle, vos collaborateurs dépendant davantage du courrier électronique pour la communication commerciale officielle et l'échange de données, le risque de fuite de fichiers confidentiels, d'éléments de propriété intellectuelle et de données sensibles augmente également.

Axway MailGate™ surveille au niveau de la passerelle Internet pour éviter que des messages et pièces jointes potentiellement dangereux n'atteignent votre réseau, et garantir que des données sensibles ne quittent pas accidentellement ou sans protection votre entreprise. Conjuguant une protection du réseau, un filtrage du contenu basé sur des règles et un cryptage automatisé dans une seule solution intégrée, MailGate protège votre réseau de messagerie de l'extérieur et de l'intérieur, réduit les tâches administratives, les coûts d'infrastructure et les responsabilités liées à une communication non sécurisée et non administrée.

Fonctionnalités clés et avantages

Protection contre les menaces externes

Réduisez la congestion du réseau et améliorez la productivité du personnel grâce à une protection antivirus, un filtrage antispam et une détection du « trafic non sollicité ».

- Détection et élimination des virus et d'autres formes de programmes malveillants avant qu'ils ne fassent des dégâts sur votre réseau
- Blocage de plus de 99 % des messages indésirables (spam) qui nuisent à la productivité du personnel, saturent le réseau et les ressources informatiques et engendrent des risques de responsabilité légale
- Protection contre les attaques de type botnet distribués avec les fonctionnalités Intelligent Edge Defense qui éliminent jusqu'à 90 % du « trafic de messagerie non sollicité » au niveau de la passerelle

Fonctionnalités clés et avantages	
<p>Sécurité des messages entrants sortants ainsi que prévention de la perte de données (DLP) Appliquez de manière universelle des règles qui protègent les données confidentielles et la propriété intellectuelle, et garantissez la conformité avec les réglementations publiques et les politiques d'entreprise</p>	<ul style="list-style-type: none"> ▪ Prévention de la perte ou la fuite de données grâce à un filtrage du contenu automatique, l'application de règles et le cryptage de passerelle à passerelle ▪ Définition et application de règles basées sur le contenu, les utilisateurs, les destinataires et les pièces jointes, qui déclenchent automatiquement des actions protectrices (par exemple, blocage, redirection ou cryptage automatique des messages) en cas d'infraction ▪ Conversion de documents MS Office contenus dans des pièces jointes en fichiers PDF protégés par des mots de passe, verrouillés et à filigrane pour en préserver l'intégrité ▪ Décrypter et vérifier l'application des politiques à tout courriel encodé S / MIME ▪ Utilisation de lexiques des domaines des services financiers, de la santé ou autres lexiques personnalisés et de filtres pour identifier les données sensibles, inadéquates et confidentielles avant qu'elles ne sortent de votre réseau ▪ Valider les signatures numériques en utilisant le Online Certificate Status Protocol (OCSP), et appliquer la politique sur les messages signés numériquement
<p>Fonctionnalités de pointe MailGate prend en charge l'ensemble des infrastructures de sécurité du courrier électronique des grandes entreprises</p>	<ul style="list-style-type: none"> ▪ Un tableau de bord d'administration intégrée, uncluster facile à déployer et une intégration transparente à n'importe quel environnement permet de mettre en œuvre MailGate rapidement ▪ La prise en charge de la multi-location permet d'appliquer des règles différentes pour plusieurs unités opérationnelles ou services dans un seul déploiement, ce qui réduit les coûts d'installation et de gestion ▪ La compatibilité IPv6 protège votre investissement alors que les secteurs public et privé décident d'adopter le nouveau protocole

Sécurité du courrier électronique complète, flexible et facile à gérer

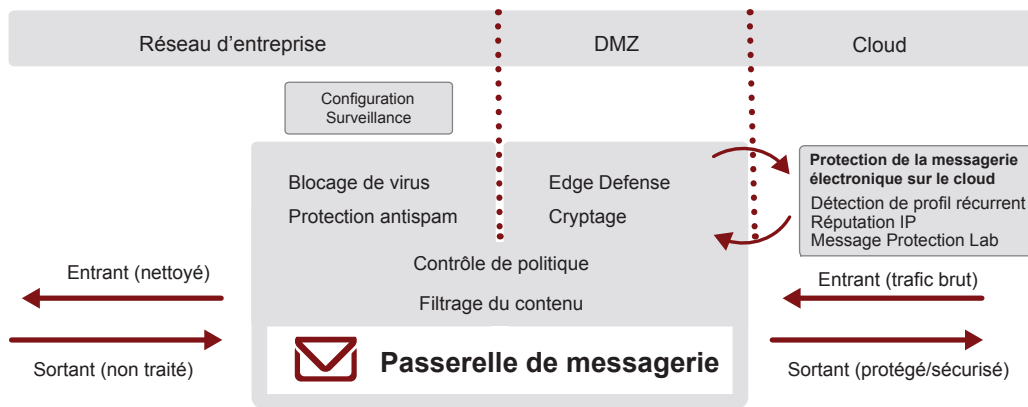
Axway MailGate fournit plusieurs couches de sécurité utilisables séparément ou conjointement pour bloquer les menaces au niveau de la zone démilitarisée (DMZ) et au sein du réseau de l'entreprise, et protéger le trafic de messagerie entrant et sortant au niveau contenu ou réseau. MailGate peut s'intégrer de manière transparente à l'architecture existante pour ajouter en toute flexibilité de nouvelles couches de sécurité selon l'évolution des besoins, sans dépendance en termes de navigateur ou de système d'exploitation et sans apporter de modifications aux systèmes d'entreprise, aux applications, aux protocoles et aux workflows des utilisateurs.

Gestion centralisée de la sécurité du courrier électronique

- MailGate permet une gestion centralisée pour accélérer son déploiement et traiter près de deux millions de messages par heure.
- Un tableau de bord de gestion performant assure une visibilité en temps réel sur le trafic de messagerie, les attaques réseau, les statistiques de spam, les files d'attente de messages, le filtrage du contenu voir plus, même entre plusieurs appliances ou environnements virtuels.
- La génération de rapports automatisée, l'exportation de données pour un reporting personnalisé et un suivi avancé des messages simplifient les tâches et améliorent la visibilité.



Axway MailGate



Antivirus

- Les moteurs sophistiqués de Kaspersky et McAfee détectent et éliminent les virus dans tous les principaux types de fichiers, notamment le code mobile et les formats de fichiers compressés.
- La mise à jour automatique des définitions de virus et du moteur permet une analyse sans interruption pour optimiser la disponibilité du système et accélérer le déploiement de remèdes.
- La protection instantanée met en quarantaine les messages et pièces jointes suspects dans les premières heures critiques d'une attaque virale.
- Définissez et appliquez des règles de protection antivirus granulaires aux utilisateurs, destinataires, types de pièces jointes et programmes exécutables.

Antispam

- Une technologie linguistique intelligente identifie le spam comme le ferait un lecteur humain et l'empêche d'atteindre le réseau.
- Déployez une protection antispam à l'échelle de l'entreprise en 30 minutes ou moins pour éliminer immédiatement plus de 99 % du spam, avec un taux de faux positifs de seulement 1 pour 100 000.
- La mise à jour des filtres configurables et des définitions de spam automatiques répond à vos besoins spécifiques.

Intelligent Edge Defense

- Détection des anomalies et réglage du débit avec des services de détection en temps réel des « zombies » et de repudiation d'adresses IP pour protéger contre les attaques de type « botnet ».
- Réduction de volume brut de courrier électronique de plus de 90 % en éliminant les attaques de pillage d'annuaire, les attaques de de type déni de service, les paquets SMTP malformés, les adresses de destinataire inexistantes et d'autres formes de messages incorrects ou malveillants.
- Vérification des destinataires au niveau du périmètre pour créer des listes de blocage et d'autorisation d'adresses IP; identifier les expéditeurs suspects et appliquer un profilage de trafic intelligent et une suppression des messages non valides.
- La technologie DKIM (Domain Keys Identified Mail) authentifie les domaines des expéditeurs de courrier électronique pour vérifier la véracité de leur identité.

Filtrage du contenu

- Exploration et analyse du contenu des messages et de plus de 300 types de pièces jointes, notamment plusieurs niveaux de fichiers d'archivage intégrés et de texte de document caché.
- Configurez des filtres à l'aide de simples cases à cocher pour identifier les données personnelles et financières, telles que les numéros de sécurité sociale ou de carte d'identité, les identifiants bancaires ou boursiers (de type CUSIP ou immatriculation des valeurs mobilières) et les numéros de carte de crédit/débit.
- Utilisez le lexique des services financiers pour détecter les données financières personnelles, notamment les relevés, les numéros de compte, les codes PIN et les confirmations d'ordre.
- Utilisez le lexique HIPAA pour rechercher des informations protégées en matière de santé, notamment des identifiants de patient, des diagnostics médicaux et procédures, des noms de médicaments et des ordonnances.

Cryptage

- Définissez des règles qui automatisent le cryptage des messages de passerelle à passerelle pour tout domaine distant.
- Appliquez des connexions TLS ou S/MIME aux domaines distants, hostnames, sites de partenaire ou adresses IP
- Recevez des alertes automatiques sur les tentatives TLS et les échecs.
- Intégrez Axway Secure Messenger pour obtenir une plate-forme de cryptage complète.

Options de déploiement

Appliance Linux renforcée

- Appliance Axway/Dell
- Appliance virtuelle VMware

Gestion des droits numériques (DRM)

- Convertissez des documents Microsoft Office sensibles en fichiers PDF protégés par un mot de passe.
- Désactivez certaines fonctions, telles que copier/coller, imprimer et modifier, pour préserver l'intégrité du contenu du document.
- Insérez un filigrane personnalisé dans des documents PDF.
- Supprimez les métadonnées et modifiez les messages sortants pour respecter la politique de l'entreprise.

Sécurité complète du courrier électronique

- Déployez Axway MailGate sur une appliance Linux renforcée et compatible avec le protocole IPv6 ainsi qu'Axway Secure Messenger, une puissante plate-forme de cryptage des e-mails entre postes de travail, afin de résoudre tous vos problèmes de sécurité de courrier électronique avec une solution complète sur une seule appliance.
- Obtenez des licences pour MailGate et Secure Messenger séparément ou simultanément. Déployez les deux solutions en même temps ou l'une après l'autre, selon l'évolution de votre entreprise.
- Un seul assistant d'installation, une seule interface d'administration et une seule interface utilisateur offrent une facilité d'installation et d'utilisation inégalée.

Haute disponibilité/Reprise d'activité

- Utilisez des fonctionnalités de reprise d'activité en cas de problème de données ou de serveur, avec un courrier électronique intact. Il est possible de restaurer les données sauvegardées.
- Utilisez un serveur de stockage NAS (Network Attached Storage) pour permettre une haute disponibilité réelle orientée application, pour une fonctionnalité transparente en cas de panne système.



Pour plus d'informations, visitez www.axway.fr
Copyright © Axway 2012. Tous droits réservés.

