Dr.WEB®

Dr.Web Mail Gateway

Meilleure qualité de filtrage du trafic de la messagerie

Référencé dans le « Registre national russe des logiciels pour les ordinateurs et les bases de données

Dr.WEB®
Dr.Web Mail Gateway

Avantages

- L'analyse des messages électroniques sans aucune restriction du côté serveur de messagerie, l'utilisation des technologies de l'analyse des messages (dont Reputation IP Filter) qui ne sont pas applicables en cas d'installation d'un système de scan du trafic sur le serveur de messagerie. Les fonctions suivantes sont disponibles sur la passerelle de messagerie :
  - La protection active contre les attaques passives et actives. Les messages malveillants peuvent être détectés selon les paramètres de la session SMTP du message et non seulement en fonction du caractère du message.
  - La détermination de l'authenticité des adresses des expéditeurs et destinataires. L'analyse des critères de spam selon l'analyse de la session SMTP.
  - La protection contre le spam dissimulé grâce à la fonction de vérification de l'authenticité de l'adresse IP.
  - La protection contre les messages mal composées (mal formés) en vérifiant les paramètres de la session SMTP.
  - La protection contre les pièges à spam.
  - La limitation des envois via les serveurs Open Relays.
  - L'économie du trafic Internet non seulement grâce à la limitation de la taille des pièces jointes mais également grâce à la possibilité d'analyser les messages lors de leur réception et avant qu'ils soient entièrement délivrés.
- L'antispam ne nécessite aucun apprentissage.
- L'augmentation de la stabilité du fonctionnement du réseau local et la réduction de la charge sur les serveurs de messagerie et les postes de travail, ceci assure leur fonctionnement normal dans le cas de croissance du nombre de messages malveillants.
- L'analyse du trafic mail par les flux multiples. Un système d'optimisation dynamique du nombre de flux d'analyse.
- Un système d'équilibrage de charge dynamique, y compris lors de l'utilisation d'un cluster.
- La réduction du coût total des licences nécessaires pour une entreprise.

Fonctionnalités clés

- L'analyse du courriel via les protocoles SMTP / LMTP / POP3 / POP3S / IMAP4 à la recherche du spam, des virus et du courrier indésirable.
- La protection contre les envois spam.
- Une garantie de livraison de messages, même si l'utilisateur n'est pas disponible pendant une longue période et qu'il ne peut pas recevoir des messages, les messages ne seront pas supprimés.
- Le filtrage du trafic conformément aux listes d'adresses blanches et noires.
- L'authentification des expéditeurs.
- L'archivage de tous les messages.
- Une configuration flexible à l'aide des règles dont la complexité peut varier, non seulement pour les différents utilisateurs et groupes, mais également pour chaque message, ce qui permet de traiter tout le courrier entrant et sortant conformément aux normes de l'entreprise et de respecter les règles de correspondance.
- Le filtrage des éléments du message par mots clé, phrases ou modèles.
- L'interface web assure la gestion de n'importe quelle partie du monde.
- La modification de messages traités selon les paramètres établis.
- L'auto-signature des messages analysés.
- Protección de funcionamiento de los módulos propios contra errores.
- La protection de ses propres modules contre le dysfonctionnement.

Licencing

Tipos de licencias

- Por el número de usuarios protegidos.
- Licencia por servidores – para el escaneo del volumen no limitado del tráfico en un solo servidor, con no más de 3 000 usuarios protegidos.

SO soportados

Distribuciones Linux de versión del núcleo 2.4.x y superior. FreeBSD de versión 6.x y superior, Solaris de versión 10 — para polataformas Intel x86 y amd64.

Fonctions	Gestion à l'aide du Centre de gestion
Traitement des protocoles POP3/SMTP/IMAP4	✓
Traitement des protocoles de messagerie sécurisés	✓
Possibilité d'installer en tant que proxy	✓
Possibilité d'utiliser dans le mode proxy transparent	✓
Possibilité d'intégrer à des systèmes de messagerie	✓
Intégration avec Active Directory/OpenLDAP	✓
Scanner antivirus	✓
Analyse antispam du trafic	✓
Blocage par types de fichiers, y compris à l'intérieur des archives	✓
Analyse antivirus du trafic	✓
Filtrage par en-têtes en utilisant des règles	✓
Modification des messages selon des règles	✓
Filtrage du trafic DoS	✓
Interdiction de transmettre des données non chiffrées	✓
Livraison garantie de tous les messages	✓
Possibilité d'utiliser plusieurs systèmes de messagerie avec des configurations différentes	✓
Procédure d'installation et mises à jour	
Traitement de messages synchrones et asynchrones	✓
Installation des modules de traitement des messages au début et à la fin de la file d'attente.	✓
Mises à jour sur demande	✓
Mises à jour automatiques	✓
Configuration de la planification des mises à jour	✓
Autres sources des mises à jour	✓
Mises à jour sur Internet/ depuis le réseau local	✓
Importation des configurations des versions antérieures	✓
Roll back des configurations	✓
Flexibilité de la sélection des politiques de sécurité	
Système de détection de spam à niveaux multiples (spam/probablement spam)	✓
Aucun besoin d'apprentissage de l'antispam, y compris chez les clients messagerie des utilisateurs	✓
Vérification des noms de domaine et des adresses IP des expéditeurs sur les listes noires externes	✓
Vérification de la présence de l'expéditeur dans la liste des domaines protégés	✓
Vérification du nom de domaine de l'expéditeur, de la présence des enregistrements A et MX et de leur correspondance aux hôtes et aux adresses IP de l'expéditeur et du destinataire	✓
Choix des adresses protégées	✓
Utilisation de listes noires et blanches des réseaux	✓
Utilisation de listes noires et blanches des domaines	✓
Listes des pièges à spam	✓
Possibilité de placer des messages en quarantaine	✓

Limitation du nombre maximal de transferts et du nombre de connexions à une adresse IP	✓
Limitation de la taille maximale du message	✓
Limitation de la taille maximale des messages reçus pendant une session	✓
Prise en charge des différents types de livraison des messages	✓
Interdiction de modifier le corps du message	✓
Limitation du nombre maximal de messages provenant d'une adresse	✓
Limitation du nombre maximal de connexions	✓
Limitation du délai pour traiter le message et ses parties	✓
Vérification de la correspondance des en-têtes à RFC-822	✓
Analyse des en-têtes et du corps du message selon des critères formels	✓
Authentification de l'utilisateur à l'aide du nom d'utilisateur et du mot de passe et de l'adresse IP	✓
Création de règles de filtrage	✓
Filtrage des éléments du message par mots clé, phrases ou modèles	✓
Filtrage des données basées par taille, types de pièces jointes, noms de fichier	✓
Configuration de critères supplémentaires de filtrage, y compris pour les messages non adressés au destinataire ou messages vides, avec des liens vers des images ou contenant des scripts	✓
Archivage et journalisation des messages	✓
Utilisation des bases de données externes	✓
Possibilité de marquer et de modifier des messages	✓
Possibilité de vérifier et d'installer une signature numérique ou un chiffrement	✓
Possibilité de transférer vers une adresse ou des adresses particulière(s)	✓
Choix d'une action à effectuer avec le message	✓
Détection et suppression des objets malveillants	
Détection et suppression des programmes malveillants de tout type, y compris dans les fichiers compressés/archives	✓
Détection des virus inconnus	✓
Détection et suppression des virus masqués sous des outils de compression inconnus.	✓
Limitation de la taille du fichier analysé	✓
Choix d'actions à appliquer aux objets infectés et suspects, ou aux objets d'un autre type	✓
Choix d'actions pour les archives contaminées	✓
Limite du niveau de compression du fichier dans l'archive, de la taille du fichier extrait à analyser	✓
Rapports et statistiques	
Recueil de statistiques sur le fonctionnement du système	✓
Configuration du niveau de détails dans les statistiques	✓
Journalisation de l'heure des événements, des objets analysés et du type d'action appliquée	✓
Génération de rapports	✓
Modification du niveau de détails des rapports	✓
Configuration de l'heure et de la périodicité d'envoi des rapports	✓
Alerte aux administrateurs et aux utilisateurs sur différents types de menaces	
Envoi des notifications à l'administrateur	✓

Utilisation des templates de notification	✓
Edition des templates de notification	✓
Utilisation des messages de contrôle	✓
Localisation	
Version du logiciel localisée	✓
Manuel d'utilisation en français (en anglais)	✓
Support technique en français	✓

DOCTOR WEB France

Адрес: 333b, Avenue de Colmar, 67100 Strasbourg

Телефон: +33 (0) 3 90 40 40 20

Факс: +33 (0) 3 90 40 40 21