



Dr.WEB®

Dr.Web Mail Gateway

Mejor calidad de filtrado del tráfico de correo

Incluido en el «Registro único de programas rusos para
ordenadores y bases de datos»

© Doctor Web S.L., 2018



Ventajas

- Escaneo de mensajes de correo sin ninguna restricción por parte del servidor de correo, uso de tecnologías de análisis de mensajes (así mismo, de Reputation IP Filter), imposibles en caso de instalación del sistema de análisis del tráfico en el servidor de correo. Solo a nivel de Gateway de correo son posibles:
 - Protección activa contra ataques pasivos y activos. Un mensaje nocivo puede ser detectado no solo por el tipo del mensaje, sino también por las opciones de la sesión SMTP de este mensaje.
 - Detección de autenticidad de direcciones de remitentes y destinatarios.
 - Análisis de características spam del mensaje a base del análisis de la sesión SMTP.
 - Protección contra spam camuflado gracias a la función de comprobación de autenticidad de la dirección IP.
 - Protección contra mensajes no creados correctamente (malformed) por medio de comprobación de velocidad de la sesión SMTP.
 - Protección contra las trampas de spam.
 - Restricción de servidores Open Relays.
 - Ahorro del tráfico de Internet no solo al restringir el tamaño de adjuntos, sino al analizar mensajes en caso de su recepción parcial.
- No hay necesidad de formación del antispam.
- Mejor estabilidad de funcionamiento de la red local y carga reducida a servidores de correo y estaciones de trabajo – posibilidad de su funcionamiento correcto en caso de aumento de mensajes nocivos.
- Escaneo multiflujo del tráfico de correo. Sistema de optimización dinámica del número de flujos de escaneo usados.
- Sistema de equilibrado dinámico de la carga, así mismo, al usar cluster.
- Reducción del precio total de licencias necesarias para la empresa.

Funciones clave

- Escaneo de mensajes de spam por protocolos SMTP/LMTP/POP3/POP3S/IMAP4 en busca de spam, virus y mensajes no deseados.
- Protección contra envíos de spam.
- Entrega garantizada de mensajes - hasta si el mensaje no está disponible durante mucho rato y no puede recibir mensajes, los mismos no se borrarán.
- Filtrado del tráfico según las listas blancas y negras de direcciones.
- Autenticación de remitentes.
- Archivado de todos los mensajes que pasan.
- Configuración flexible usando reglas de complejidad aleatoria - no solo para varios usuarios y grupos, sino para cada mensaje, lo que permite procesar todo el correo entrante y saliente en función de estándares corporativos, controlar la conformidad con las normas de correspondencia.
- Filtrado de elementos de mensajes por palabras clave, frases o plantillas.
- Administración a través de la interfaz web desde cualquier lugar del mundo.
- Modificación de mensajes procesados en función de la configuración.
- Autofirma de mensajes de correo escaneados. Estadísticas que toman en cuenta todos los aspectos de funcionamiento del sistema.
- Protección de funcionamiento de los módulos propios contra errores.

Dr.Web Mail Gateway es:

Protección de la información confidencial El producto le permite recuperar mensajes borrados accidentalmente por los usuarios desde sus buzones de correo, así como para realizar investigaciones relacionadas con la filtración de información.

Solución abierta. Dr.Web Mail Gateway puede ser integrado en soluciones de otros productores, y gracias a API abierta, se puede añadir las nuevas posibilidades funcionales al mismo.

Licencias

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 plataformas Intel x86 y amd64.

Opciones de licencias

Licencia básica		Componentes adicionales Dr.Web	
Antivirus	Antispam	SMTP proxy	Centro de control (se licencia de forma gratuita)

Funcionalidad	Administración en el CC
Procesamiento de protocolos de correo POP3/SMTP/IMAP4	✓
Procesamiento de protocolos de correo protegidos	✓
Posibilidad de instalación como Proxy	✓
Posibilidad de usar en modo de proxy "transparente".	✓
Posibilidad de integración en sistemas de correo	✓
Integración con Active Directory/OpenLDAP	✓
Disponibilidad del escáner antivirus en el producto	✓
Escaneo antispam del tráfico	✓
Bloqueo por tipos de archivos, así mismo, dentro de archivos	✓
Escaneo antivirus del tráfico	✓
Filtrado por encabezados usando reglas	✓
Modificación del mensaje usando reglas	✓
Filtrado del tráfico DoS	✓
Prohibición de transmisión de datos no cifrados	✓
Entrega garantizada de todos los mensajes de correo	✓
Trabajo con varios sistemas de correo con diferente configuración	✓
Instalación y actualizaciones	
Procesamiento de mensajes síncrono y asíncrono	✓
Instalación de los módulos de procesamiento al principio y al final de la cola de procesamiento	✓
Actualizaciones por demanda	✓
Actualizaciones automáticas	✓
Configuración de la programación de actualizaciones	✓
Fuentes alternativas de actualizaciones	✓
Actualizaciones desde Internet/LAN	✓
Importación de configuraciones de versiones anteriores	✓
Reversión de la configuración	✓
Flexibilidad al seleccionar las políticas de seguridad informática	
Sistema multinivel de detección de spam (spam/posiblemente spam)	✓
No es necesario formar el antispam, asimismo, a través de Clientes con usuarios	✓
Comprobación de los nombres de dominios y direcciones IP de remitentes por listas negras externas	✓
Comprobación para ver si el remitente forma parte del listado de dominios protegidos	✓
Comprobación del nombre del dominio del remitente, de presencia y correspondencia de entradas DNS A- y MX a hots y direcciones IP del remitente y destinatario	✓
Selección de direcciones protegidas	✓
Uso de listas negras y blancas de redes	✓
Uso de listas negras y blancas de dominios	✓
Listas de trampas de spam	✓
Posibilidad de mover los mensajes a cuarentena	✓

Restricción del número máximo de reenvíos, del número de conexiones con una dirección IP	✓
Restricción del tamaño máximo del mensaje	✓
Restricción del tamaño máximo de mensajes recibidos en una sesión	✓
Soporte de varios tipos de entrega de mensajes	✓
Prohibición de cambio del cuerpo del mensaje	✓
Restricción del número máximo de mensajes desde una dirección	✓
Restricción del número máximo de conexiones	✓
Restricción del periodo de procesamiento del mensaje y sus partes	✓
Comprobación de encabezados para ver si corresponden a la especificación RFC-822	✓
Análisis de encabezados y del cuerpo por características formales	✓
Autorización del usuario por nombre y contraseña, dirección IP	✓
Creación de reglas de filtrado	✓
Filtrado de elementos de mensajes por palabras clave, frases o plantillas	✓
Filtrado de datos por tamaño, tipos de adjuntos, nombre del archivo	✓
Configuración de características extra de filtrado, así mismo, para mensajes no destinados al remitente que tienen enlaces a imágenes que contienen scripts	✓
Archivado y registro de mensajes	✓
Uso de bases de datos externas	✓
Posibilidad de marcar y modificar mensajes	✓
Posibilidad de comprobar e instalar la firma digital, el cifrado	✓
Posibilidad de reenviar a la dirección o direcciones determinadas	✓
Selección de acciones con el mensaje	✓
Detección y eliminación de objetos nocivos	
Detección y eliminación de programas nocivos de cualquier tipo, así mismo, dentro de archivos comprimidos/archivados	✓
Detección de virus desconocidos	✓
Detección y eliminación de los virus ocultos por empaquetadores desconocidos	✓
Restricción del tamaño del archivo escaneado	✓
Selección de acciones para objetos infectados, sospechosos y de otro tipo	✓
Selección de acciones para archivos infectados	✓
Restricción del grado de compresión en el archivo, del tamaño del archivo descomprimido que debe ser escaneado	✓
Informes y estadísticas	
Generación de estadísticas sobre el funcionamiento del sistema	✓
Configuración de nivel de detalle de estadísticas	✓
Posibilidad de registrar la hora del evento, el objeto de escaneo y el tipo de acción	✓
Generación de informes	✓
Cambio del nivel de detalle de informes	✓
Configuración de la hora y periodicidad de envío de informes	✓
Notificación a administradores y usuarios sobre amenazas de varios tipos	
Envío de notificaciones al administrador	✓

Envío de plantillas de notificaciones	✓
Edición de plantillas de notificaciones	✓
Uso de mensajes administrativos	✓
Localización	
Versión localizada del programa	✓
Guía de usuario en ruso	✓
Soporte técnico en ruso	✓

Doctor Web, S.L.

Doctor Web es un productor ruso de los medios de seguridad informática. Los productos antivirus Dr.Web se desarrollan a partir del año 1992.

125040, Rusia, Moscú, c/3 Yamskogo Polya, 2, edificio 12a

Teléfono: +7 495 789-45-87 (multicanal), Fax: +7 495 789-45-97

[антивирус.пф](#) | www.drweb.ru | www.av-desk.com | <http://free.drweb.ru> | <http://pda.drweb.com>