Características Clave

- **Protección contra Falsos Positivos**—porque nadie se beneficia cuando un correo se identifica erróneamente como spam o inseguro, las herramientas de la aplicación aseguran la entrega de mensajes legítimos.
- **Detección de amenazas ocultas**—Múltiples pruebas de seguridad, incluyendo múltiples plug-ins de antivirus, proporcionan protección de nivel empresarial contra amenazas ocultas, tanto entrantes como salientes.
- **Diseño Flexible**—Porque las medidas de seguridad del futuro serán diferentes de las de hoy, la flexibilidad en su diseño protege su inversión en software por los años venideros.
- **Acceso Vía Web**—El gateway es fácilmente accesible tanto para administradores como para usuarios, a través de su interfase web.
- **Listas Negras y Listas blancas**—Los mensajes entrantes de servidores en Listas negras siempre son rechazados. Los mensajes entrantes de servidores incluídos en Listas Blancas pueden opcionalmente pasar sin algunas validaciones.
- **Listas específicas por usuario**—Los usuarios pueden especificar sus propias Listas Negras y Blancas.
- **Bitácoras de Mensajes**—Las Bitácoras para administradores y usuarios muestran el proceso de cada correo—entregado, en cuarentena, rechazado—y porqué.
- **Reportes Gráficos**—Cuenta con reportes gráficos en tiempo real que revelan tendencias del correo. Cada reporte contiene puntos seleccionables ligados a las bitácoras de mensajes.
- **Pruebas para Puesta a punto**—Se pueden realizar ajustes a la agresividad de cada prueba ya sea globalmente o por dominios individuales.

SecurityGateway
For Exchange/SMTP Servers

Defensas en capas y configuración flexible mejoran el desempeño y seguridad del servidor.

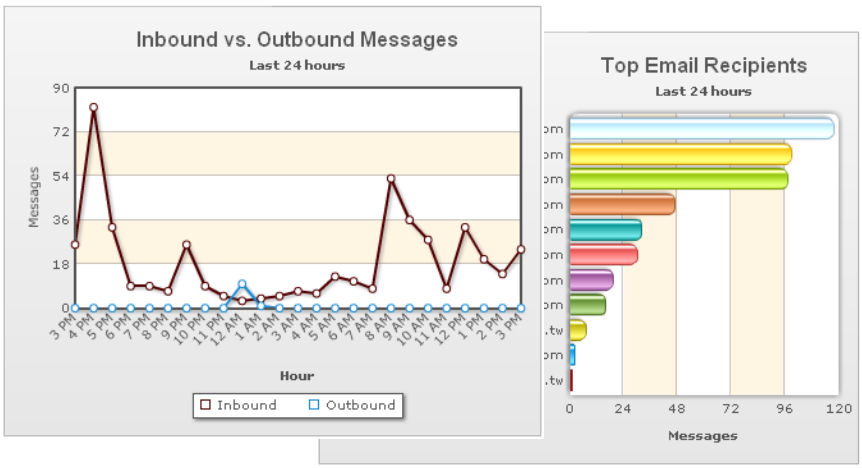
SecurityGateway para Exchange/SMTP combina más de una década de experiencia en brindar seguridad para el correo electrónico con tecnologías de seguridad probadas para proteger el tráfico de correo de ataques maliciosos, modificación de mensajes y robo de identidades de direcciones de correo electrónico; enfocado a organizaciones que utilizan Microsoft Exchange® o cualquier otro servidor SMTP.

Utilizando múltiples métodos de seguridad, SecurityGateway para Exchange/SMTP asegura la entrega precisa de correo legítimo al mismo tiempo que minimiza los posibles falsos positivos.

SecurityGateway para Exchange/SMTP ofrece protección flexible con parámetros de configuración sencillos y fáciles de usar y administrar. Su diseño de seguridad en capas, protege a las empresas contra amenazas en el correo entrante y saliente negando a spammers y hackers la posibilidad de ataques.

Los clientes que desean múltiples motores antivirus y protección proactiva contra dispersiones pueden agregar el plug-in ProtectionPlus. ProtectionPlus amplía y complementa las características integradas de SecurityGateway combinando un reconocimiento adicional de firmas y análisis heurístico para detectar virus, spam, phishing, spyware y otros tipos de correo no deseado y malicioso.

ProtectionPlus
For SecurityGateway



SecurityGateway para Exchange/SMTP proporciona múltiples reportes gráficos.

alt-n technologies
Trusted Messaging Solutions

Beneficios principales

Administración Sencilla. Su interfase intuitiva y orientada a la tarea permite a los administradores realizar acciones comunes con un mínimo esfuerzo. Las responsabilidades administrativas se pueden delegar al administrador del dominio. Es posible habilitar a los usuarios finales para determinar el destino de sus mensajes sin necesidad de contactar al administrador.

Poderoso Filtrado. SecurityGateway para Exchange/SMTP cuenta con un poderoso motor de filtrado basado en el lenguage de filtrado de correos SIEVE, estándar de la industria. El Administrador puede ampliar la funcionalidad de SecurityGateway para Exchange/SMTP con sus propios scripts SIEVE.

Detección Precisa. Con múltiples herramientas de análisis para separar las amenazas, del correo legítimo, SecurityGateway detiene virtualmente todo el correo problemático, permitiendo que las comunicaciones de la empresa sean más eficientes.

Prevención de pérdida de datos. Su interfase amigable permite crear políticas para dar soporte a la inspección del contenido saliente. Las reglas de filtrado pueden ayudar a detectar y prevenir envíos no autorizados de información sensible hacia afuera de su red.

Protección de su Inversión. Incluye un año de Actualizaciones, proporcionando las nuevas versiones del producto durante el periodo de Protección.

Requerimientos del Sistema

- Computadora con procesador Pentium 4 (Se recomienda procesador multi core).
- Mínimo 512 MB de memoria (2 GB recomendados).
- Sistema Operativo Microsoft Windows Vista/XP/2000/2003 .
- Tarjeta de Red.
- Protocolo TCP/IP instalado.
- Disco NTFS con mínimo 500 MB de espacio disponible.
- Navegadores Firefox 1.5, Internet Explorer 6.0, Opera 8.5, o Safari. Adobe Flash Player 8.0 o superior para visualizar gráficos.

SecurityGateway Configuración y Características

Opciones de Seguridad

Anti-Spam
- Heurístico y Bayesiano
- Bloqueo de listas de DNS
- Bloqueo de listas de URL´s
- Listas grises
- Certificación de Mensajes
- Protección contra retrodispersiones (Backscatter)
- Puntuación de Mensajes
- Protección contra dispersiones a través de ProtectionPlus

Anti-Virus
- Actualización automática de firmas
- Múltiples motores vía ProtectionPlus

Anti-Spoofing
- Búsquedas inversas
- Verificación y firmas DKIM
- Validación de SPF
- SenderID
- Verificación de cuentas del correo entrante

Anti-Abuso
- Control de Relay
- Autenticación de SMTP
- Protección de IP
- Monitoreo dinámico
- Tarpitting
- Bandwidth Throttling

Filtrado
- Reglas de filtrado de contenido de mensajes
- Tipos de archivo predeterminados

Listas Negras
- Direcciones
- Hosts
- Direcciones IP
- Acciones por Lista Negra

Listas blancas
- Direcciones
- Hosts
- Direcciones IP

Políticas
- Reglas de filtrado SIEVE

Opcional - ProtectionPlus
- Motor Antivirus de Kaspersky
- Protección contra dispersiones vía análisis de patrones en tiempo real

Opciones de Configuración

Dominios y Usuarios
- Creación/Mantenimiento automático de Dominios y usuarios
- Múltiples Dominios de Correo
- Administradores de Dominio
- Configuración de Opciones por usuario

Manejo del Correo
- Múltiples Dominios por Servidor de Correo
- Opciones configurables de entrega de correo

Opciones de Cuarentena
- A nivel Dominio para Administradores
- Acceso a nivel Usuario

Mantenimiento de la Base de Datos
- Respaldo y Restauración

Bitácoras del Sistema

Bitácoras de Mensajes
- Bitácoras Globales de Mensajes
- Bitácoras de Mensajes por Dominio
- Mensajes en Cuarentena

Bitácoras Históricas
- Retención configurable de archivos históricos
- Imagen de bitácora del Sistema
- Imagen de la bitácora del correo entrante
- Imagen de la bitácora del correo saliente
- Imagen de la bitácora del acceso HTTP

Reportes

Resúmen
- Múltiples opciones de filtrado
- Graficado en tiempo real
- Desglose analítico de correo basura
- Utilización de ancho de banda

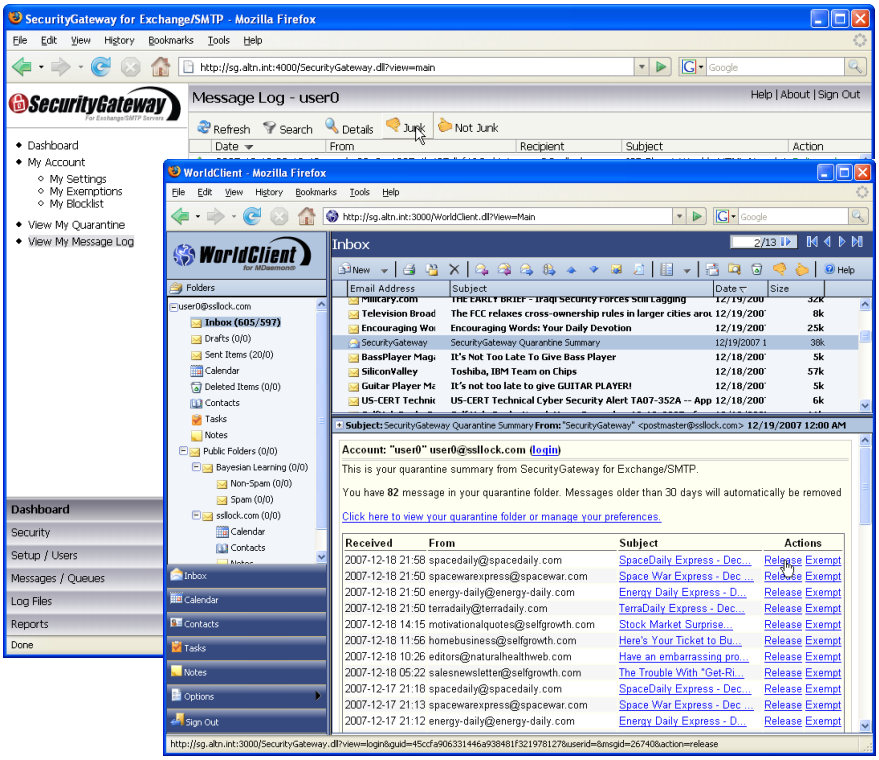
Correo Entrante
- Mensajes Procesados
- Principales receptores de correo
- Principales receptores por tamaño

Correo Saliente
- Mensajes Procesados
- Principales Emisores
- Principales Emisores por tamaño

Anti-Spam
- Principales emisores por Dominio
- Principales Receptores

Anti-Virus
- Entrantes capturados
- Entrantes por Nombre
- Salientes capturados
- Salientes por nombre

Opciones de Cuentas Privadas
- Parámetros de Procesamiento
- Listas Negras y Listas Blancas
- Bitácoras de Mensajes
- Manejo de la Cuarentena



Cumbre: Usuarios específicos pueden tener acceso a sus bitácoras de mensajes y realizar tareas tales como identificar el spam.

Fondo: Se envía a los usuarios un correo informando de mensajes en Cuarentena, permitiéndoles liberar los mensajes de la Cuarentena o agregar a Lista Blanca al emisor.

Trusted Messaging Solutions

2550 SW Grapevine Parkway,
Suite 150 Grapevine, Texas 76051
Phone: (817) 601-3222
Fax: (817) 601-3223

www.altn.com

09.08.2008