

**FaceTime** esta de acuerdo a Gartner en el cuadrante mágico de administración de Instant Messenger, además de administrar P2P, filtrado URL y detección y alivio de spyware, tráfico también llamado GREYNET.

Las soluciones de FaceTime permiten a las empresas dar seguridad y control sobre las redes con aplicaciones evasivas (greynets). El manejo efectivo de estas greynets ayuda a prevenir la infección de spyware, bloquear P2P y administrar el uso legítimo de IM para:

- ▶ Proteger la tecnología y la propiedad intelectual.
- ▶ Hacer cumplir los requerimientos regulatorios y corporativos.
- ▶ Optimizar el valor del negocio de sistemas existentes.
- ▶ Incrementar la productividad del empleado y reducir costos.

Solo FaceTime ofrece una profunda defensa, una estrategia comprensiva para la seguridad punto-a-punto, cumplimiento de normas y administración de greynets.



**Tráfico GreyNet en las empresas**

IM	
ANONYMIZERS	
WEB CONFERENCING	
FILE SHARING	
VIDEO STREAMING	
VOIP	
WEB BROWSING	

**Antecedentes**

Los sitios de trabajo han crecido de manera global y son distribuidos.

Una comunicación y colaboración efectiva constituyen los ingredientes clave para mantener un éxito y crecimiento de negocios globales. Por más de una década, el correo electrónico (e-mail) sirvió a este propósito. Pero su naturaleza fuera de línea y los tiempos de retraso inherentes al e-mail dieron la pauta para el crecimiento de la mensajería instantánea (IM).

El e-mail hoy en día, casi ha sido remplazado por el IM como el medio de comunicación y colaboración mas aceptado debido a su naturaleza dinámica.

La habilidad para ver si alguien esta en línea e iniciar una conversación instantánea es demasiado útil para ser ignorado.

Aunado a esto, hay una multitud de usos como conferencias en línea, llamadas PC-a-PC, llamadas PC-a-Teléfono, compartir archivos y transferencias de archivos, conversaciones encriptadas de texto y voz y salas de chat.

La infraestructura tradicional de seguridad como los cortafuegos soportan únicamente capa 4 y solo pueden bloquear las direcciones IP y números de puertos destino usado por las aplicaciones. Son incapaces de identificar amenazas potenciales y tomar una acción correctiva ya que no analizan el tráfico de red que pasa a través de ellos.

Las aplicaciones GreyNet como el spyware, IM y P2P pueden pasar por un firewall sin ser detectadas ya que cambian sus direcciones IP y puertos frecuentemente (port crawling). Estas aplicaciones también pueden usar puertos y direcciones IP legales (permitidas) para evadir la detección y el bloqueo del firewall.

## FaceTime RTGuardian



Real-Time Guardian (RTG) es la solución mas avanzada de seguridad perimetral para administrar la navegación web, aseguramiento de IM y P2P no autorizados y bloqueo del extensión de malware en la empresa. RTGuardian se integra con FaceTime IMAuditor (IMA) para formar la solución líder de la industria en materia de Seguridad en IM. Con FaceTime GreyNet Enterprises Manager (GEM), RTGuardian forma una solución de puerta de enlace con seguridad Web. RTG permite el uso seguro y productivo de Internet incluyendo navegación web, IM, P2P y otras aplicación de comunicación en tiempo real.

RTGuardian provee una solución total de seguridad para empresas que se topan con amenazas que evolucionan constantemente y el uso irresponsable de Web. Cuando se coloca en el perímetro de la red el RTGuardian complementa los cortafuegos corporativos:

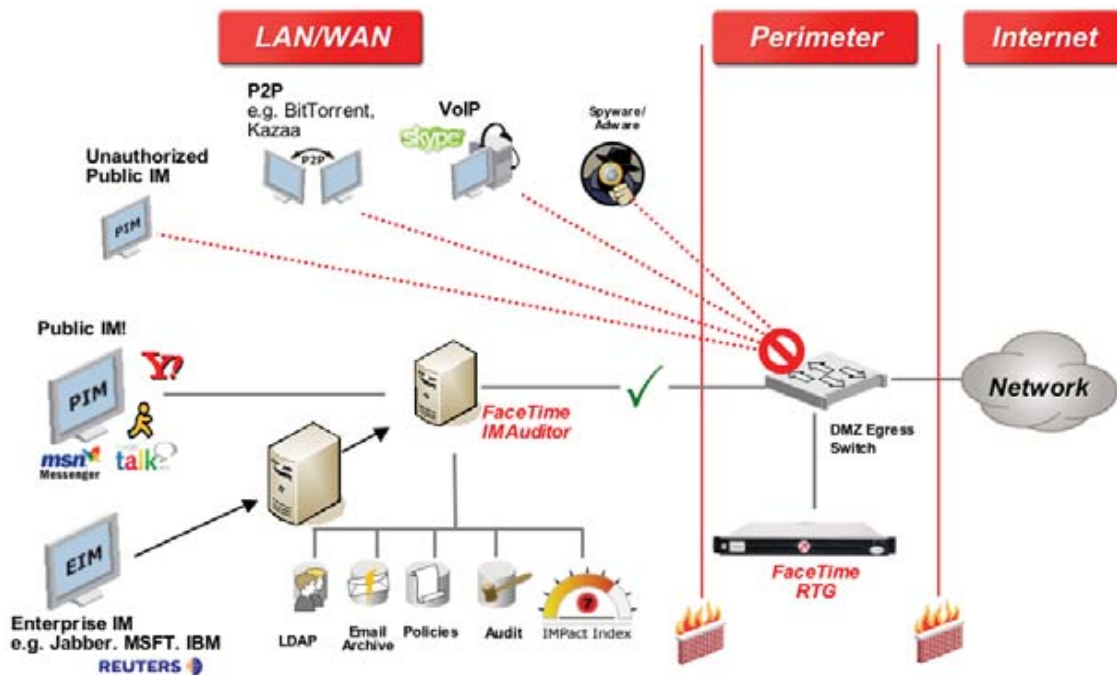
- ▶ Para identificar spyware, IM y aplicaciones P2P por medio de una inspección profunda de los paquetes para comparar y analizar patrones de diversos protocolos.
- ▶ Para bloquear aplicaciones basándose en políticas configurables
- ▶ Para proveer mayor información en los patrones de uso de Internet de los empleados.

## Beneficios

- Refuerza la política corporativa del uso de Web por medio de categorías y filtros url.
- Analiza protocolos al nivel de la aplicación y realiza una profunda inspección de los paquetes.
- No hay impacto en el desempeño de la red ya que no es parte del flujo del tráfico de la red.
- Ofrece una instalación práctica ya que no requiere cambios en la infraestructura de la red actual.
- Detiene a los usuarios que visitan sitios comunes de infección de spyware y adware y bloquea la descarga de tipos conocidos de spyware.
- Provee seguridad a los datos de la empresa de los spywares que recaban información antes de que deje la red corporativa.
- Identifica computadoras infectadas con algún tipo de spyware para su pronta recuperación.
- Soporta protocolos de redes IM como AIM/ICQ, MSN, Reuters, Yahoo!, IMRelay, American Idol, Jabber, Google Talk y QQ.
- Soporta una gran variedad de protocolos P2P para compartir archivos como FastTrack, KaZaA, Gnutella, Morpheus, Limewire, Bearshare, eDonkey, SoftEther y Winny.
- Soporta Skype, el protocolo emergente de VoIP/IM P2P
- Bloquea acciones no seguras del cliente de IM, como conexiones directas, transferencias de archivos e imágenes, así como conexiones de voz y video.

- Bloquea el cambio de puertos (port crawling) y túneles (tunneling) de clientes IM.
- Provee una interfase basada en Web para su administración y monitoreo.

### RTGuardian instalado en una LAN



### Argumentos Promocionales

- Maneja políticas granulares.
- Muestra gráficas de uso de los servicios (actualizadas cada 10 minutos).
- Resetea el origen.
- Utiliza protocolo ICAP\*.
- Decodifica sesiones de IM encriptadas con secway
- Soporta capa 7 e identifica versiones de las aplicaciones.
- Bloquea SpIM (Spam over Instant Messaging) y SpIT (Spam over Internet Telephony)

\*El Protocolo de Adaptación de Contenidos de Internet (o ICAP, del inglés Internet Content Adaptation Protocol) es un protocolo de red abierto y público, originado en 1999 para la redirección de contenidos con fines de filtrado y conversión. Estandarizado en Abril de 2003 como RFC 3507. Permite el uso de antivirus, filtrado de contenidos, traducción dinámica de páginas, inserción automática de anuncios, compresión de HTML, etc. Los servicios basados en ICAP tienen dos posibilidades de implantación, dependiendo de si la redirección al servidor de filtrado se realiza inmediatamente después de la solicitud del cliente (modo "request") o tras la respuesta del servidor de destino (modo "response"). Normalmente se asocia el filtrado de acceso al modo solicitud y el filtrado de contenido al modo respuesta.

### Dimensionamiento

Espec. del Hardware	RTG110	RTG550	RTG1100	RTG2000
Modelo Base	PE 860	PE 860	PE 1950	PE 1950
CPU	Pentium D Pro 915- 2.8 GHz	Xeon 3070 Dual core, 2.66 GHz	2 x Dual core Xeon Pro 5110, 1.6 GHz	2 x Dual core Xeon Pro 5160, 3 GHz
FSB	800 MHz	1066 MHz	1066 MHz	1333 MHz
Memoria	2GB	2 GB	4 GB	4 GB
HDD	80 GB	80 GB	2 x 73 GB (RAID)	2 x 73 GB (RAID)
Red	2 X 10/100/1000	2 X 10/100/1000	3 X 10/100/1000	3 X 10/100/1000
Otro	CD	CD	DVD + Dual power	DVD + Dual power
Tipo de aplicacion	Low-end	Mid-Range	High-End	High-End
# Usuarios	100-400	100-1500	1000-4500	1000-4500
<b>Rendimiento con Filtrado Web y Spyware</b>				
# Max HTTP Hits/sec	500	700	1750	>2000

Rendimiento (Mbps)	88	108	245	>318
<b>Rendimiento sin Filtrado Web</b>				
# Max HTTP Hits/sec	600	920	2600	?
Rendimiento (Mbps)	98	150	370	?
<b>Rendimiento sin Filtrado Web y Spyware</b>				
Rendimiento (Mbps)	150	205	410	?

## FaceTime IMAuditor



IMAuditor es la solución líder de clase empresarial para la seguridad, la administración, cumplimiento de normas y control de la mensajería instantánea y de otros usos de comunicación en tiempo real.

IM es el medio de comunicaciones electrónicas de crecimiento más rápido en la historia; la presencia es el tono de marcar de hoy, y las empresas están derivando claramente la ventaja significativa de la comunicación rápida y eficaz. Pero la utilización creciente de los programas IM públicos y empresariales está planteando las amenazas de seguridad de entrada y de salida que pueden dar lugar a brechas de seguridad, la pérdida de la productividad y fugas de información.

### Beneficios

#### Seguridad

- Analiza los archivos transferidos, incluyendo transferencias LCS, usando los antivirus existentes.
- Opera como Proxy invisible para evitar que el malware deshabilite la protección y esconda la dirección IP
- Bloqueo zero-day de ataques de worms y virus usando canales de comunicación en tiempo real.
- Bloqueo de SpIM (Spam en IM) usando una combinación de listas para permitir/denegar, filtrado de contenido y respuesta de frase (challenge).
- Bloquea transferencias de archivos, o permite transferencias con limites de tamaño impuestos.
- Previene pérdidas de propiedad intelectual e información confidencial ruteando las comunicaciones de los empleados sobre redes IM publicas internamente y bloqueando mensajes usando palabras en una lista que soporta patrones avanzados de palabras y expresiones regulares completas.

#### Cumplimientos de normas

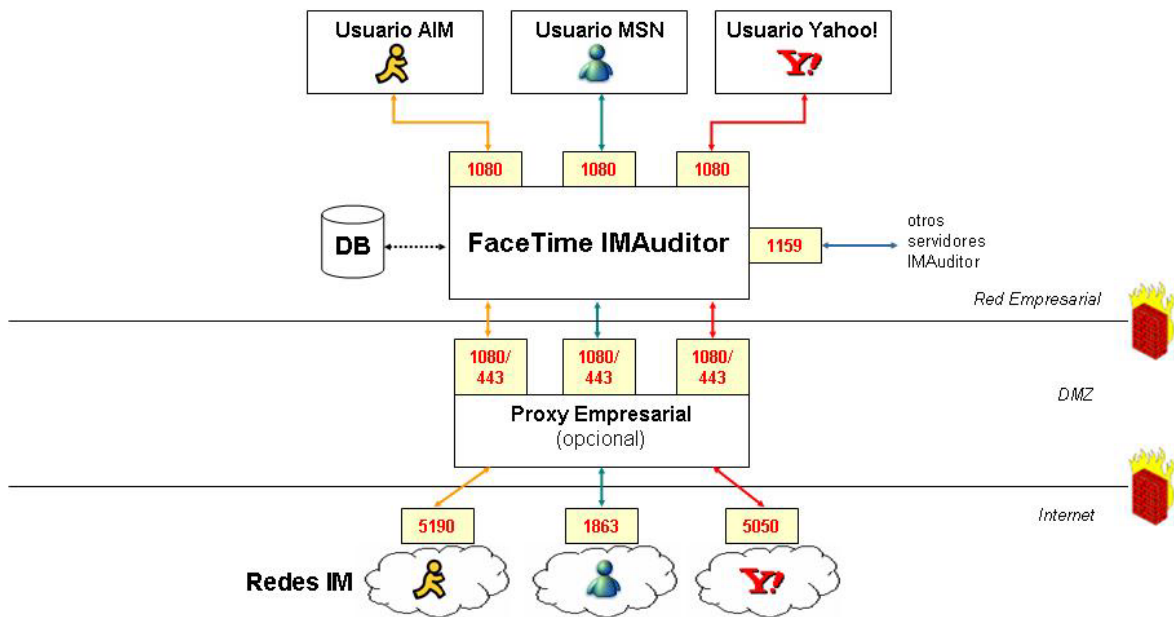
- Archiva las transferencias de archivos en redes empresariales de IM.
- Reporte de conversaciones conducidas sobre clientes de IM.
- Almacenamiento binario de todas las comunicaciones en tiempo real, incluyendo un historial de entradas y salidas del usuario así como platicas multi-usuario, 100% garantizado.
- Despliegue automático de disclaimers (mensajes legales) personalizados para todos los involucrados en la conversación.
- Asignar y aplicar el cumplimiento de normas regulatorias a nivel de la compañía, grupo o individuos.
- Facilita la segregación de roles y tareas basado en las responsabilidades funcionales del individuo.
- Configura políticas de 'Paredes Chinas' para restringir el contacto entre grupos.
- Maneja un flujo de proceso sofisticado para el monitoreo de contenidos, ciclos de revisión y consultas con búsquedas personalizadas.
- Integración completa con sistemas comunes de e-mail y almacenamiento WORM.
- Previene modificación de mensajes con una marca de impresión horaria, asegurando conversaciones registradas coinciden con las conversaciones exportadas.
- Notificaciones y alertas por e-mail para asegurar la retención de registros y facilitar la recuperación.

#### Administración y Control

- Administra transferencias de archivo, colaboración (conferencias audio/video, VoIP) y otros privilegios del cliente a nivel de compañía, grupo y usuario para todos los servicios de comunicación en tiempo real.
- Asocia la ID de empleado en el directorio corporativo con sus cuentas de IM (buddy names)
- Accesos de control basados en IP

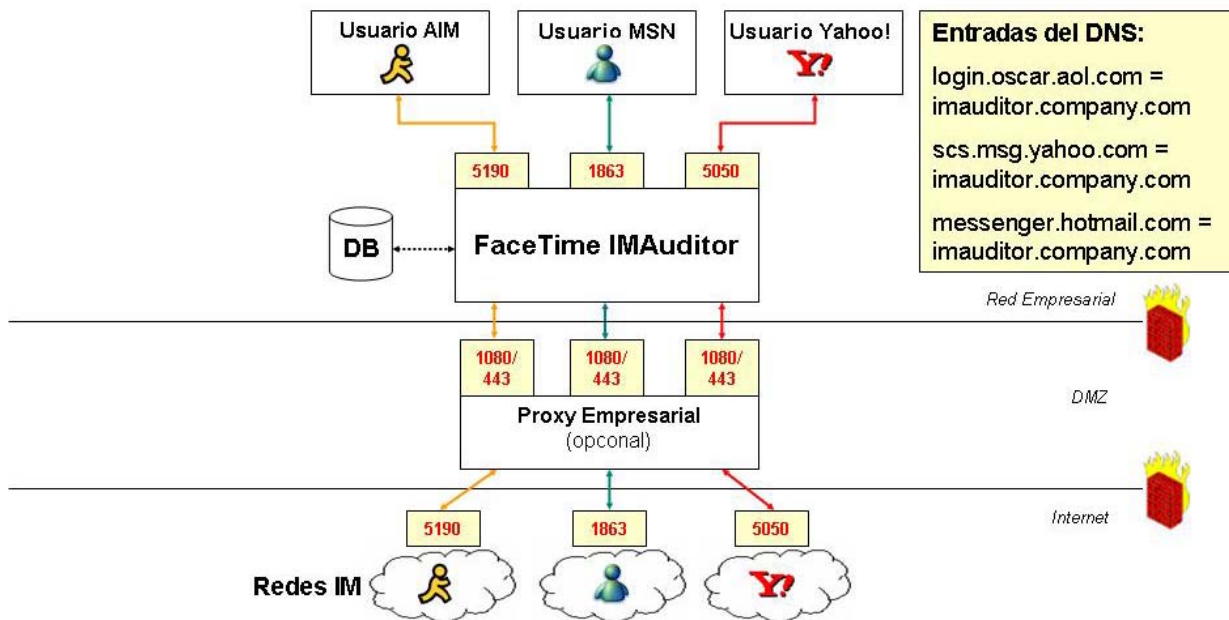
- Reportes de uso en tiempo real y graficas con estadisticas.
- Acceso por medio de una interfase basada en web segura e intuitiva.
- Controles avanzados para clientes de IM corporativos para una mejor experiencia del usuario.

### IMAuditor en modo SOCKS Proxy



El tipo de conexión por SOCKS proxy requiere que los clientes de IM sean configurados para apuntar explícitamente al IMA como servidor proxy.

### IMAuditor en modo DNS



El ruteo por DNS requiere modificaciones en tu servidor DNS, pero los clientes de IM usan sus configuraciones por defecto (default) y no requieren configuración adicional.

## FaceTime GEM

GEM permite a las organizaciones administrar las políticas de seguridad y agregar reportes del tráfico para IM, P2P y spyware a través de ambientes distribuidos. Al integrarse con RTGuardian, GEM se convierte en una solución de red para anti-spyware que tiene como objetivo la remediación y reparación de puntos de infección sin necesidad de instalar un programa cliente.

### Beneficios

#### Instalación

- No requiere aplicación cliente.

#### Políticas Anti-Spyware

- Las políticas son usadas para determinar las actividades preventivas a realizar sobre un grupo de computadoras.

#### Remediación del Objeto

- La remediación consiste en dos fases; remover la infección existente e inocular los clientes contra futuras infecciones.

### GEM y RTGuardian

