

# STSMailsSafeAppliance

DISPOSITIVO PARA LA ELIMINACIÓN DE SPAM  
Y VIRUS DEL CORREO ELECTRÓNICO  
DOCUMENTACIÓN TÉCNICA DICIEMBRE 2008



Tel.Fax: 966 446 046  
[www.soltecsis.com](http://www.soltecsis.com)  
[comercial@soltecsis.com](mailto:comercial@soltecsis.com)

# STSMailsSafeAppliance

## ÍNDICE

1. INTRODUCCIÓN .....	04
2. ARQUITECTURA .....	06
2.1. STS-MAILSAFE APPLIANCE EN MODO CLUSTER.....	08
3. STS-MAILSAFE ENGINE .....	10
3.1. TECNICAS ANTISPAM .....	11
3.2. MOTORES ANTIVIRUS SOPORTADOS .....	13
3.3. STS-MAILSAFE MILTER .....	14
4. INTERFAZ DE USUARIO .....	18
4.1. MONITORIZACIÓN .....	19
4.2. ADMINISTRACIÓN .....	21
4.3. INFORMES ESTADÍSTICOS .....	21

# STSMAILS SAFE APPLIANCE

## 1. INTRODUCCIÓN



# STSMAILS SAFEAPPLIANCE

## 1. INTRODUCCIÓN

En el presente documento se describen las características técnicas más sobresalientes del dispositivo **STS-MAILSAFE APPLIANCE** diseñado y suministrado por la empresa **SOLTECSIS SOLUCIONES TECNOLÓGICAS, S.L.** como una solución de gran eficiencia y eficacia para la supresión del spam y virus de los mensajes de correo electrónico analizados a través del mismo.

El **STS-MAILSAFE APPLIANCE** se utiliza como un elemento intermedio entre el flujo de correo destinado a un conjunto de dominios y el servidor o conjunto de servidores en los cuales se encuentran almacenados los buzones de dichos dominios. La función del mismo es la de limpiar de spam y virus los mensajes antes su entrega en los buzones destino.

Para la identificación del spam se utilizan de forma combinada las técnicas más avanzadas existentes hoy en día.

El dispositivo permite utilizar gran variedad de motores antivirus, tanto comerciales como no comerciales. Es posible incluso hacer uso de varios motores antivirus de forma simultánea con el fin de aumentar la capacidad de supresión de virus.

Existe la opción de una configuración cluster formada por dos o más nodos **STS-MAILSAFE APPLIANCE** gracias a la cual es posible escalar de un modo sencillo el sistema con la finalidad de soportar cualquier volumen de mensajes, así como garantizar la continuidad del servicio prestado aunque se produzca cualquier tipo de avería en uno de los nodos que forman el cluster.

La monitorización y administración del **STS-MAILSAFE APPLIANCE** se lleva a cabo a través de una sencilla interfaz gráfica basada en entorno web.

# STSMAILS SAFE APPLIANCE

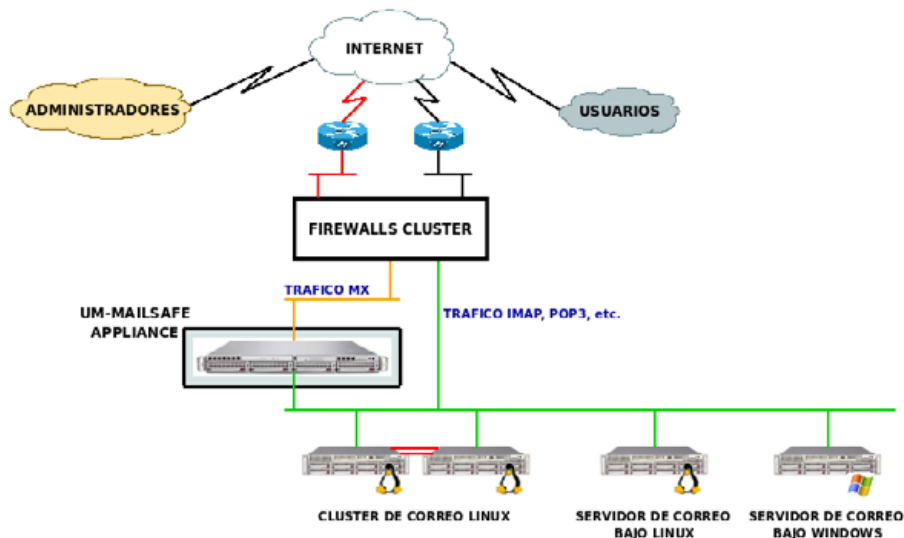
## 2. ARQUITECTURA



# STSMAILSAPPLIANCE

## 2. ARQUITECTURA

En el diagrama que se muestra a continuación se puede apreciar la ubicación típica que el dispositivo **STS-MAILSAFE** suele tener en el interior de las infraestructuras de una empresa.



Como se puede apreciar, el **STS-MAILSAFE** recibe todo el tráfico de correo destinado a los distintos servidores de correo existentes en la empresa, limpiando de spam y virus el mismo antes de proceder a su entrega final en el buzón del correspondiente servidor destino.

Los servidores de correo a los cuales el **STS-MAILSAFE** entrega los mensajes limpios pueden ser cualquier tipo de servidor que acepte la entrega de mensajes mediante protocolo SMTP. Por lo tanto, el dispositivo es capaz de limpiar el correo para cualquier tipo de servidor de correo, **independientemente del servidor de correo en cuestión y del sistema operativo** sobre el cual se instale este.

El **STS-MAILSAFE** se comporta como un **enrutador de correo electrónico**, enrutando el correo, una vez limpio de spam y virus, a su correspondiente servidor de correo para el almacenamiento del mismo en el buzón del destinatario.

El dispositivo es **capaz de enrutar tanto a nivel de dominio como a nivel de buzón**. A través de la interfaz de administración del dispositivo es posible gestionar la tabla de rutas de correo de tal modo que podemos crear rutas por dominio y por buzón. Es decir, podemos hacer que el dispositivo entregue el correo limpio destinado a un conjunto de dominios a un cierto servidor, e incluso hacer que los correos destinados a un conjunto de buzones vayan a un servidor predeterminado.

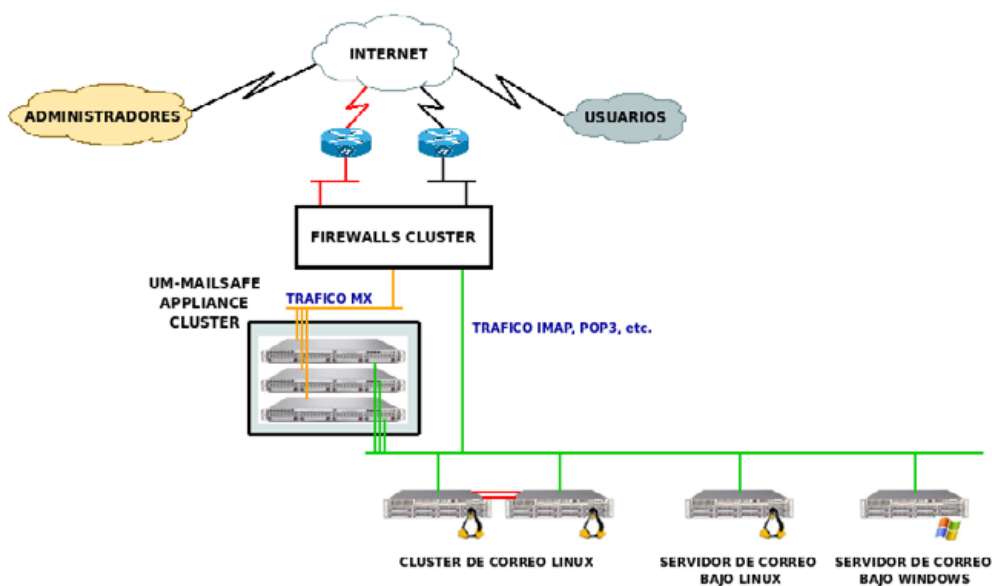
# STSMAILS SAFEAPPLIANCE

## 2. ARQUITECTURA

El enrutamiento a nivel de buzón puede ser útil para diseminar los buzones de uno o varios dominios entre servidores distintos, con el fin de repartir la carga y espacio entre distintos servidores. Una cosa a tener en cuenta en el enrutamiento a nivel de buzón es que el servidor que permite el acceso al usuario final a su buzón (mediante protocolo POP3, IMAP, etc) tiene que ser capaz de saber en que servidor se encuentra ubicado el buzón del usuario.

### 2.1. STS-MAILSAFE APPLIANCE EN MODO CLUSTER.

Con el fin de dotar de características de **ALTA ESCALABILIDAD** y **ALTA DISPONIBILIDAD** al dispositivo **STS-MAILSAFE**, es posible configurar este como una granja de frontales MX para **funcionar en modo cluster** tal y como se muestra en el siguiente diagrama.



Gracias a esto, es posible añadir tantos nodos al cluster como sea necesario para soportar la carga creciente de tráfico de correo, así como evitar que el **STS-MAILSAFE** deje de funcionar aún cuando se produzca cualquier tipo de avería (tanto hardware como software) en uno de los nodos del cluster, dado que en tal caso, siempre disponemos de otro nodo que garantizará la continuidad del servicio mientras se solventa el problema surgido en el nodo averiado.

Como veremos en la sección 4 del presente documento, el dispositivo **STS-MAILSAFE** integra una sencilla y potente interfaz para la monitorización y administración del mismo.

Desde esta interfaz se tiene un control muy preciso de la carga que está soportando el dispositivo en parámetros claves como la CPU, memoria, red, disco, etc.

# STSMAILS SAFEAPPLIANCE

## 2. ARQUITECTURA

A través de las gráficas de estado del módulo de monitorización podemos saber fácilmente si el dispositivo es capaz de soportar toda la carga de correo o es necesario añadir más nodos al cluster. Es más, la información obtenida es tan valiosa y precisa que permite anticiparnos para añadir con antelación suficiente más nodos al cluster antes de que el sistema alcance un punto de sobrecarga crítico.

En la configuración cluster del **STS-MAILSAFE** la interfaz de monitorización y administración se instala en uno solo de los nodos del cluster. Desde la misma se gestionan todos los nodos de forma transparente para el administrador de sistemas.

La adición de un nuevo nodo al cluster es una operación que se lleva a cabo de un modo sencillo a través de la interfaz de usuario. Una vez añadido el mismo a través de esta interfaz, configuraciones comunes a todos los nodos (tablas de rutas de correo, listas blancas, listas negras, etc.) son replicadas de inmediato en el nuevo nodo.

Una cosa importante a tener en cuenta en la configuración cluster es que debe de existir algún mecanismo de balanceo de carga que permita repartir el tráfico de correo entrante (tráfico MX) entre los distintos nodos del cluster.

Esto se puede llevar a cabo mediante el servicio DNS, pero supone tener que asignar una IP pública a cada uno de los nodos del cluster. Es más recomendable utilizar un firewall con capacidades de balanceo de carga. El sistema de firewalls **UM-FireWall** descrito en el documento anexo **UM-FireWall.pdf** dispone de tales capacidades de balanceo de carga, entre otras muchas más.

# STSMAILS SAFE APPLIANCE

## 3. STS-MAILSAFE ENGINE



# STSMAILSAPPLIANCE

## 3. STS-MAILSAFE ENGINE

El motor antivirus/antispam utilizado por el **STS-MAILSAFE APPLIANCE**, al cual denominaremos **STS-MAILSAFE ENGINE**, se sirve de **las más avanzadas técnicas** existentes hoy en día tanto para la identificación de mensajes spam como para la supresión de virus en el correo electrónico.

El **STS-MAILSAFE ENGINE** es una herramienta de enorme **eficiencia** (consume pocos recursos del sistema, gracias a lo cual es posible soportar mayor carga de correo con un mismo dispositivo) y **eficacia** (tiene un elevadísimo índice de identificación de spam y virus) que permite la supresión de prácticamente todos los mensajes spam y/o infectados por virus antes de que estos puedan llegar a los buzones de los usuarios a los cuales van destinados.

### 3.1. TECNICAS ANTISPAM.

Como ya se ha resaltado, el **STS-MAILSAFE ENGINE** se sirve de las técnicas más avanzadas existentes hoy en día en lo que a materia antispam se refiere. De entre dichas técnicas cabe destacar las siguientes:

- Bases de datos **ORDB** (Open Relay Data Base). Estas bases de datos son accesibles desde Internet y listan IPs desde las cuales se ha detectado envío de spam de forma masiva. Como veremos más adelante en la sección correspondiente al **STS-MAILSAFE MILTER**, es posible rechazar mensajes provenientes de IPs de spammers en la fase inicial de conexión al servicio MX. Es decir, si la IP de origen está incluida en una de estas bases de datos, se rechaza la conexión antes de que se empiece a recibir un solo byte del mensaje que se pretende entregar en la plataforma de correo, con el correspondiente ahorro tanto de ancho de banda como de tiempo de proceso del mensaje.
- **SPF** (*Sender Policy Framework*). Consiste en una configuración DNS, que un dominio dado puede tener o no activa, mediante la cual se restringe el conjunto de servidores desde los cuales se pueden enviar correos con remitentes pertenecientes al dominio en cuestión. Mediante esta técnica es posible rechazar correos cuyo remitente pertenece a un dominio con la configuración SPF activa. Si la IP desde la cual proviene el mensaje no está dentro de la lista de IPs permitidas, el mensaje se rechaza. Al igual que el mecanismo descrito en el párrafo anterior, esta técnica la implementa directamente el **STS-MAILSAFE MILTER**, de tal modo que si un correo es rechazado por SPF se evita recibir un solo byte del mensaje con el correspondiente ahorro tanto de ancho de banda como de tiempo de proceso.
- Mecanismos de *checksums* (firmas digitales) **DCC**, **Pyzor** y **Razor**. Estos mecanismos permiten generar un valor de firma digital para el e-mail que está siendo analizado comparándolo posteriormente con bases de datos de firmas de mensajes spam existentes en Internet. Si la firma generada del mensaje que está siendo analizado se encuentra en una de estas bases de datos, dicho mensaje tiene una probabilidad muy alta de ser spam. Es lo que se conoce como **Hash Sharing System**. Cada uno de estos módulos (DCC, Pyzor y Razor) se sirve de sus propias bases de datos en Internet y su modo de funcionar y generar las firmas digitales difiere. La combinación de los tres módulos constituye una potente ayuda en la identificación de spam.

# STSMAILS SAFEAPPLIANCE

## 3. STS-MAILSAFE ENGINE

- Bases de datos probabilísticas **Bayes** con mecanismos de autoaprendizaje que permiten aumentar la eficacia en la identificación de spam a medida que el sistema va aprendiendo por su cuenta. A través de la interfaz de usuario es posible inyectar mensajes en dicha base de datos para mejorar el índice de spam detectado.

- **Fuzzy OCR**. Muchos de los mensajes spam suelen tener adjunta una imagen en la cual se detalla el producto objeto del spam, en vez de hacerlo en el propio texto del mensaje, con el fin de eludir las comprobaciones llevadas a cabo por los sistemas de identificación de spam. El sistema antispam implementado en el **STS-MAILSAFE ENGINE** incluye un módulo *Fuzzy OCR* (*Optical Character Recognition*) que permite extraer el texto de las imágenes adjuntas para identificar si se trata o no de mensajes spam. Para acelerar este proceso se dispone de mecanismos que generan una base de datos de firmas digitales de imágenes de tal modo que si entra un nuevo mensaje spam con una imagen analizada previamente con su firma en la base de datos, directamente es marcado como spam. Esto es de enorme utilidad para ahorrar tiempo de proceso, dado que los mecanismos OCR suelen requerir de bastantes recursos tanto de CPU como de memoria.

- **URIDNSBL**. Este plugin es de gran ayuda en la detección de mensajes spam dado que sirve para identificar URLs correspondientes a sitios web que se considera contienen información de spammers. Cuando en un mensaje aparece una URL, esta se compara con bases de datos con URLs pertenecientes a spammers y, en caso de existir, se genera la puntuación correspondiente para aumentar la probabilidad de que el mensaje sea identificado como spam.

- **DomainKeys**. Mediante este plugin es posible validar aquellos e-mails que contengan firmas del tipo *DomainKeys*. Este sistema de firma sirve para validar la identidad del usuario que envía el e-mail, sirviéndose de la criptografía de clave pública/clave privada. La clave pública se almacena en el DNS del dominio del remitente, en un registro TXT.

- **Bases de reglas dinámicas**. Se trata de varias bases de reglas utilizadas para analizar la estructura y contenido de los mensajes, actualizadas diariamente de forma automatizada, y que ayuda en gran medida a aumentar la eficiencia del sistema de detección de spam.

El **STS-MAILSAFE ENGINE** se sirve de todas estas técnicas y de muchas más para la generación de una puntuación a través de la cual es posible discernir si un mensaje es o no spam. Cada test llevado a cabo sobre el mensaje da a este una mayor o menor puntuación que concluye en una puntuación final que determinará si el mensaje es considerado o no como spam.

A través de la interfaz de usuario es posible fijar el valor de puntuación a partir de cual se considera que un mensaje es spam. Es posible incluso fijar un valor de puntuación alto a partir del cual se considera que el mensaje es spam seguro (*high spam*) y hacer que este se borre directamente sin llegar al buzón final.

# STSMailsafeAppliance

## 3. STS-MAILSAFE ENGINE

### 3.2. MOTORES ANTIVIRUS SOPORTADOS.

El **STS-MAILSAFE ENGINE** permite la utilización de varios motores antivirus de forma simultánea con el fin de aumentar al máximo posible la eficacia del sistema antivirus.

Gracias a esto conseguimos que la plataforma esté preparada lo más pronto posible para combatir una infección por un nuevo virus, dado que cuantos más motores antivirus utilicemos más probable será que tengamos más pronto la firma para el mismo, debido a que unas empresas tardan más que otras en incorporar nuevos virus a sus bases de datos de firmas.

Prácticamente todos los motores antivirus soportados disponen de mecanismos para la actualización automatizada de las bases de datos de firmas.

A continuación se pasa un listado de los motores antivirus soportados. Como se puede ver, el abanico es bastante amplio cubriendo tanto motores opensource como motores comerciales:

- sophos ..... ([www.sophos.com](http://www.sophos.com))
- mcafee ..... ([www.mcafee.com](http://www.mcafee.com))
- command ..... ([www.command.co.uk](http://www.command.co.uk))
- bitdefender ..... ([www.bitdefender.com](http://www.bitdefender.com))
- drweb ..... ([www.dials.ru/english/dsav\\_toolkit/drwebunix.htm](http://www.dials.ru/english/dsav_toolkit/drwebunix.htm))
- kaspersky ..... ([www.kaspersky.com](http://www.kaspersky.com))
- etrust ..... (<http://www3.ca.com/Solutions/Product.asp?ID=156>)
- inoculate ..... ([www.cai.com/products/inoculateit.htm](http://www.cai.com/products/inoculateit.htm))
- inoculan ..... ([ftp.ca.com/pub/getbbs/linux.eng/inoclar.LINUX.Z](ftp://ca.com/pub/getbbs/linux.eng/inoclar.LINUX.Z))
- nod32 ..... ([www.nod32.com](http://www.nod32.com))
- f-secure ..... ([www.f-secure.com](http://www.f-secure.com))
- f-prot ..... ([www.f-prot.com](http://www.f-prot.com))
- panda ..... ([www.pandasoftware.com](http://www.pandasoftware.com))
- rav ..... ([www.ravantivirus.com](http://www.ravantivirus.com))
- antivir ..... ([www.antivir.de](http://www.antivir.de))
- clamav ..... ([www.clamav.net](http://www.clamav.net))
- trend ..... ([www.trendmicro.com](http://www.trendmicro.com))
- norman ..... ([www.norman.de](http://www.norman.de))
- css ..... ([www.symantec.com](http://www.symantec.com))
- avg ..... ([www.grisoft.com](http://www.grisoft.com))
- vexira ..... ([www.centralcommand.com](http://www.centralcommand.com))
- symscanengine ... ([www.symantec.com](http://www.symantec.com))
- avast ..... ([www.avast.com](http://www.avast.com))

# STSMAILSAPPLIANCE

## 3. STS-MAILSAFE ENGINE

### 3.3. STS-MAILSAFE MILTER.

Un *milter* (*Mail Filter*) es un programa que interactúa con el MTA (*Mail Transfer Agent*) en las diferentes etapas por las que pasa un mensaje a medida que este va llegando al MTA.

En el **STS-MAILSAFE APPLIANCE** existe un MTA (el **STS-MAILSAFE MTA**) encargado de recibir todo el correo de entrada y un milter (el **STS-MAILSAFE MILTER**) con el cual interactúa el MTA para aumentar la eficiencia del sistema antispam del modo en que vamos a describir a continuación.

El **STS-MAILSAFE MILTER** se convierte un elemento clave del dispositivo **STS-MAILSAFE** dado que supone un **ahorro considerable tanto en ancho de banda como en potencia de proceso** debido a que permite rechazar mensajes spam antes de que los bytes que los constituyen sean recibidos.

Si nos fijamos en el RFC que describe el protocolo SMTP veremos que existen varias fases por las que hay que pasar antes de poder enviar un mensaje a un MTA.

En primer lugar tenemos el inicio de la conexión TCP sobre el MTA al cual se va a mandar el mensaje. El **STS-MAILSAFE MILTER** se puede configurar para que analice la IP desde la cual se está iniciando conexión sobre el **STS-MAILSAFE MTA**. Si esta IP aparece en alguna de las listas ORDB (*Open Relay Data Bases*) utilizadas se puede rechazar directamente la conexión evitando así la entrada de mensajes spam desde dicha IP sin recibir un solo byte de dichos mensajes.

En la siguiente fase del protocolo SMTP es necesario indicar un remitente mediante el comando: `MAIL FROM:<email_del_remitente>`

En este punto es posible hacer que el **STS-MAILSAFE MILTER** analice la configuración DNS del dominio del remitente para ver si el SPF (*Sender Policy Framework*) está activo. En caso de que sí se puede comprobar si la IP de la conexión entra dentro del rango de IPs permitidas. En caso de que no se rechaza la conexión sin que entre un solo byte del mensaje.

En esta fase, el **STS-MAILSAFE MTA** es también capaz de rechazar remitentes no válidos, por ejemplo, porque el dominio del remitente indicado no exista.

En la siguiente fase del protocolo SMTP se especifica la lista de destinatarios del mensaje mediante varios comandos del tipo: `RCPT TO:<email_del_destinatario>`, uno por cada destinatario.

Se puede configurar el **STS-MAILSAFE MILTER** para que por cada destinatario que se va indicando se analice si el buzón destino existe o no, si dispone de cuota para albergar un nuevo mensaje, si en sus correspondientes listas ACLs (*Access Control Lists*) existe alguna regla que impida la entrada del mensaje en curso (por ejemplo, que el e-mail o dominio del remitente aparezca en una lista negra creada por el propietario del buzón), etc. De nuevo, si existe algo que conlleve la no aceptación del mensaje, este se rechaza sin que entre un solo byte del mismo a la plataforma de correo.

# STSMAILS SAFEAPPLIANCE

## 3. STS-MAILSAFE ENGINE

En relación a lo que se ha explicado en el párrafo anterior hay una cosa que hay que tener muy presente y es el hecho de que, dado que los buzones no se encuentran físicamente en el propio **STS-MAILSAFE APPLIANCE** sino que se encuentran repartidos por los diversos sistemas de correo que este puede estar protegiendo en un momento dado, es necesario un mecanismo que permita comunicar con el servidor de correo final al cual va destinado un mensaje para verificar si el buzón destino existe, si dispone de cuota, si existe alguna ACL que impida la entrega del mensaje en dicho buzón, etc.

Dado que los sistemas de correo que protege el **STS-MAILSAFE APPLIANCE** pueden ser muy diversos y funcionar tanto bajo diferentes sistemas operativos como pueden ser el Linux o el Windows, lo que se hace es instalar un agente en cada sistema de correo con el cual se comunica el **STS-MAILSAFE MILTER** para llevar a cabo las comprobaciones indicadas.

A este agente lo vamos a denominar **STS-MAILSAFE AGENT**. Se trata de un proceso servidor que se ejecuta en cada sistema de correo protegido por el **STS-MAILSAFE APPLIANCE** y que atiende peticiones de servicio en un puerto TCP. La comunicación entre este y el **STS-MAILSAFE MILTER** se lleva a cabo de forma encriptada y además es posible hacer que el **STS-MAILSAFE AGENT** restrinja las conexiones en función de la IP de origen.

Dada la amplia diversidad de sistemas de correo que existen hoy en día, resulta prácticamente inviable programar el **STS-MAILSAFE AGENT** para que sea capaz de cubrir todos los posibles sistemas y configuraciones con el fin de llevar a cabo la función que acabamos de describir. En vez de esto, lo que hace el **STS-MAILSAFE AGENT** es ejecutar un **programa local** (el cual puede ser un shell script en Linux, un archivo de procesamiento por lotes en Windows, etc.) el cual se encarga de indicar en última instancia si el buzón existe o no, si dispone de cuota, si hay definida alguna ACL que conlleva el rechazo del mensaje entrante, etc.

Este programa local se crea en base al sistema de correo subyacente y el sistema operativo sobre el cual se ejecuta este. Las comprobaciones que lleva a cabo pueden ser tan simples como verificar si existe un directorio o un fichero para validar la existencia o no de un buzón.

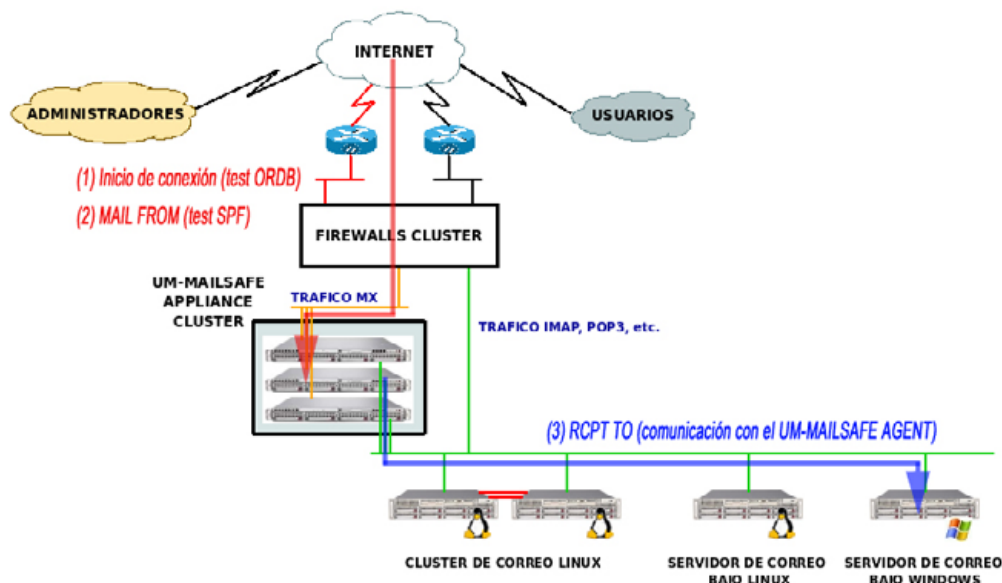
El **STS-MAILSAFE AGENT** analiza el código de respuesta retornado por el programa local y, en función del mismo, retorna el código correspondiente para indicar al **STS-MAILSAFE MILTER** si el buzón existe o no, si tiene su cuota agotada, si hay alguna ACL que impida la entrada del mensaje que está siendo analizado, etc.

Hay que tener muy presente la notable versatilidad que este programa local proporciona, dado que nos permite programarlo a nuestro antojo en función de las capacidades y características del sistema de correo en el cual se instala el **STS-MAILSAFE AGENT**.

# STSMAILSAPPLIANCE

## 3. STS-MAILSAFE ENGINE

Con el fin de entender mejor el modo de comunicación entre el **STS-MAILSAFE MILTER** y el **STS-MAILSAFE AGENT**, veamos a continuación un gráfico explicativo de todo el proceso.



(1) En primer lugar, el **STS-MAILSAFE MTA** recibe un inicio de conexión desde Internet a través de la cual se pretende entregar un mensaje de correo electrónico a uno de los sistemas de correo protegidos. Nada más recibir la conexión, el **STS-MAILSAFE MTA** comunica con el **STS-MAILSAFE MILTER** para que este lleve a cabo el test ORDB con el fin de ver si la IP de origen de la conexión existe en alguna de las bases de datos de IPs de spammers. En caso de que sí, dicha conexión se rechaza inmediatamente.

(2) En caso de que no, el **STS-MAILSAFE MTA** continúa la comunicación con el cliente hasta que este hace uso del comando **MAIL FROM** para indicar el e-mail del remitente. El **STS-MAILSAFE MTA** comunica de nuevo con el **STS-MAILSAFE MILTER** para que este lleve a cabo la comprobación SPF sobre el dominio del remitente. Si el dominio tiene activada la configuración SPF y la IP de la conexión no se encuentra dentro del rango de IPs permitidas, se rechaza la conexión.

(3) Si el test SPF se supera con éxito, por cada comando **RCPT TO** recibido, el **STS-MAILSAFE MTA** establece comunicación con el **STS-MAILSAFE MILTER** el cual comunica a su vez con el **STS-MAILSAFE AGENT** del sistema de correo que alberga el buzón del destinatario. Este lanza el script local a través del cual se decide si el mensajes es aceptado o rechazado por razones tales como no existir el buzón destino, no disponer de cuota, alguna ACL que conlleve el rechazo del remitente, etc. El **STS-MAILSAFE AGENT** transfiere la respuesta generada por el script local al **STS-MAILSAFE MILTER** para que este acabe aceptando o rechazando el mensaje según se indique en el código de respuesta recibido.

# STSMAILS SAFEAPPLIANCE

## 3. STS-MAILSAFE ENGINE

Veamos a continuación un simple ejemplo para ver de un modo más claro el enorme ahorro que el **STS-MAILSAFE MILTER** puede suponer. Imaginemos un intento de envío masivo de mensajes spam con imágenes adjuntas a miles de buzones albergados en los sistemas de correo protegidos.

Si la IP de origen desde la cual se envían estos mensajes spam aparece en una ORDB, ninguno de estos mensajes llegaría a entrar, dado que serían rechazados de inmediato.

Si no se dispusiera del proceso **STS-MAILSAFE MILTER**, los mensajes entrarían en el **STS-MAILSAFE APPLIANCE** con el correspondiente consumo de ancho de banda y acabarían siendo procesados por el **STS-MAILSAFE ENGINE** con el correspondiente consumo de CPU, disco, etc.

# STSMAILS SAFE APPLIANCE

## 4. INTERFAZ DE USUARIO



# STSMAILS SAFEAPPLIANCE

## 4. INTERFAZ DE USUARIO

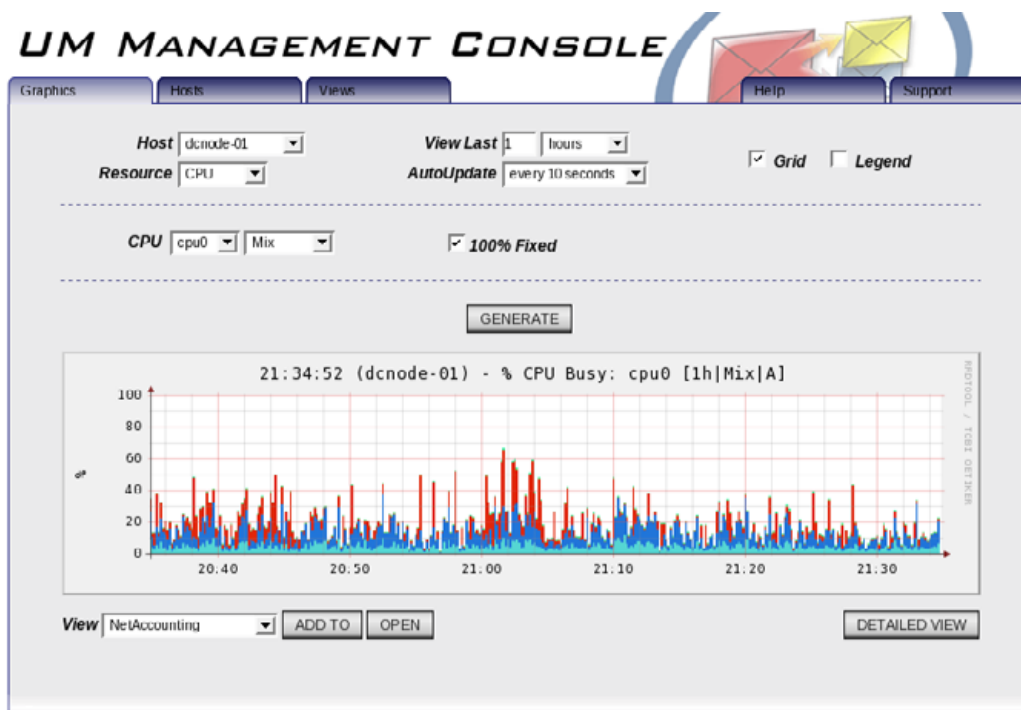
Como se ha indicado a lo largo del documento, el **STS-MAILSAFE APPLIANCE** dispone de una interfaz de usuario que permite administrar de un modo sencillo tanto una configuración con un solo nodo, como una configuración cluster con múltiples nodos.

En la configuración en cluster, esta interfaz se instala en uno sólo de los nodos del cluster y desde ella se administran todos los nodos que componen el cluster.

### 4.1. MONITORIZACIÓN.

La interfaz dispone de una sección de monitorización a través de la cual es posible ver con sumo detalle y precisión el estado de cada uno de los nodos **STS-MAILSAFE**. La monitorización se lleva a cabo a través del módulo *Monitor* del sistema **SOLTECSIS MANAGEMENT CONSOLE**. Este es un sistema muy eficaz que permite generar gráficas de estado de los recursos (CPU, memoria, carga de disco, tráfico de red, etc.) de todos los equipos con datos muy precisos que permiten identificar con facilidad si alguno de los nodos está empezando a saturarse, la carga que está soportando la plataforma, etc.

A continuación se puede apreciar una captura de pantalla de esta interfaz en la que se muestra la carga de CPU de un nodo clasificada por colores (el rojo tiempo de I/O, el azul oscuro ocupación de CPU en modo usuario, el azul claro ocupación de CPU en modo sistema, etc.).



# STSMAILS SAFE APPLIANCE

## 4. INTERFAZ DE USUARIO

Se trata de una herramienta de enorme utilidad dado que permite monitorizar con gran precisión el estado de la plataforma y llevar a cabo ampliaciones a tiempo para evitar posibles saturaciones en los servicios prestados a los usuarios.

En la sección 8 del documento adjunto **UM-Firewall.pdf** se puede ver una explicación muy detallada de esta herramienta junto con varias capturas de pantalla que muestran las gráficas de estado generadas así como la apariencia y potencia del entorno de monitorización.

Para tener un control en tiempo real del estado de todos los servicios y recursos de la plataforma, se instala también el sistema de monitorización **Nagios**, gracias al cual vamos a poder monitorizar que los servicios de todos los equipos del sistema están operativos así como controlar el estado de los recursos (por ejemplo, si una partición de disco está apunto de llenarse, si la cantidad de procesos en memoria es excesiva, si hay demasiados mensajes en cola, etc.).

Este sistema permite la generación de alertas por e-mail o SMS, incluso el escalado de alertas para si una avería no se solventa en un tiempo predeterminado se escale a otros operadores.

A continuación se muestra una captura de pantalla en la que se muestra como se puede controlar desde el Nagios el estado de un conjunto de servidores.

**Current Network Status**  
Last Updated: Fri Jan 11 11:49:36 CST 2008  
Updated every 90 seconds  
Nagios® 3.0rc1 - www.nagios.org  
Logged in as nagiosadmin

**Host Status Totals**

Up	Down	Unreachable	Pending
17	0	0	0

**Service Status Totals**

OK	Warning	Unknown	Critical	Pending
169	4	0	2	0

**Service Overview For All Host Groups**

**Environmental Probes (environmental-probes)**

Host	Status	Services	Actions
vers01v	UP	2 OK	[Icons]
temetraxa1	UP	3 OK 2 WARNING	[Icons]

**Fedora Core 8 Production Servers (fc8-production-servers)**

Host	Status	Services	Actions
dev1	UP	33 OK 1 WARNING 1 CRITICAL	[Icons]
fltr	UP	42 OK	[Icons]
task	UP	37 OK 1 CRITICAL	[Icons]

**Printers (printers)**

Host	Status	Services	Actions
hp42906en	UP	2 OK	[Icons]
hp4290	UP	2 OK	[Icons]

**Production Linux Servers (production-linux-servers)**

Host	Status	Services	Actions
dev1	UP	31 OK 1 WARNING 1 CRITICAL	[Icons]
fltr	UP	42 OK	[Icons]
narman	UP	3 OK	[Icons]
task	UP	37 OK 1 CRITICAL	[Icons]

**Production Websites (production-websites)**

Host	Status	Services	Actions
ivaymon.com	UP	6 OK	[Icons]
nagios.com	UP	6 OK	[Icons]
nagios.org	UP	6 OK	[Icons]
nagioscommunity.org	UP	6 OK	[Icons]

**Switches (switches)**

Host	Status	Services	Actions
linksys-sne224n	UP	1 OK	[Icons]

# STSMAILSAFEAPPLIANCE

## 4. INTERFAZ DE USUARIO

### 4.2. ADMINISTRACIÓN.

A parte de la monitorización de estado, desde la interfaz de usuario vamos a poder gestionar la configuración del dispositivo **STS-MAILSAFE**, tanto en su configuración de único nodo como en su versión cluster.

A través del módulo *STS-MAILSAFE* de la *SOLTECSIS Management Console* vamos a poder llevar a cabo acciones tales como:

- Administración de la lista de dominios que van a ser procesados por el dispositivo.
- Gestionar la tabla de rutas de correo para indicar que sistemas de correo albergan los buzones para un cierto dominio de tal modo que el dispositivo sepa donde tiene que entregar los mensajes. El enrutamiento se puede llevar a nivel de buzón. Se puede establecer una ruta por defecto correspondiente a un servidor al cual van dirigidos todos aquellos mensajes para los cuales no se haya establecido una ruta específica.
- Definir a nivel de dominio o buzón si se llevan o no a cabo los análisis antivirus y/o antispam.
- Gestión de listas blancas y listas negras.
- Fijar los valores de puntuación umbrales a partir de los cuales se considera que un mensaje es spam y a partir del cual se considera spam con alto grado de puntuación (*high spam*).
- Inyectar mensajes spam y no spam para entrenar el sistema de bases de datos probabilísticas Bayes.
- Añadir nuevos nodos a una configuración cluster.

### 4.3. INFORMES ESTADÍSTICOS.

El **STS-MAILSAFE APPLIANCE** dispone de un potente módulo para la generación de informes estadísticos de e-mail, el cual es a su vez capaz de ayudar a atajar spam de forma dinámica en función de los resultados obtenidos a partir de dichos informes.

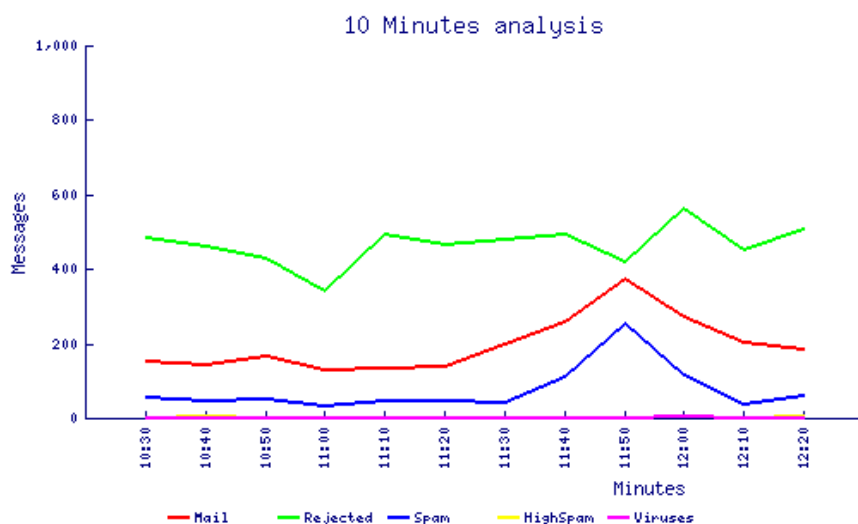
Para atajar el spam se utiliza un mecanismo dinámico que es capaz de cortar de forma radical envíos masivos de spam desde una IP dada en un tiempo razonable y con una heurística muy sencilla.

Si el sistema de análisis de logs detecta que se han recibido más de *n* mensajes spam desde una misma IP a lo largo de un plazo de tiempo preestablecido, dicha IP será añadida de modo automático a una base de datos de listas negras para que se rechacen conexiones desde la misma. Permanecerá en esta base de datos durante un periodo mínimo preestablecido, pudiendo ampliarse el mismo si el envío de spam persiste después del periodo de bloqueo.

# STSMailsSafeAppliance

## 4. INTERFAZ DE USUARIO

Veamos a continuación a través de un caso real la eficacia de este sencillo mecanismo antispam. La gráfica que se muestra a continuación corresponde a una de las secciones del informe generado por el módulo de análisis de logs.



Este gráfico muestra en color verde todo el e-mail directamente rechazado por el **STS-MAILSAFE MTA** por alguna de las otras razones que hemos explicado en la sección correspondiente al **STS-MAILSAFE MILTER**. En color rojo se representan los mensajes procesados por el **STS-MAILSAFE ENGINE**. Del total de mensajes procesados, en color azul se representan los que son spam, en amarillo los que son *high spam* y en lila los que contenían virus.

Como se puede apreciar en el gráfico de ejemplo, aproximadamente a las 11:30h se empieza a detectar un aumento considerable tanto en el correo procesado (color rojo) como en el número de mensajes identificados como spam (color azul). Este incremento se continúa apreciando en ejecuciones sucesivas del módulo generador de informes hasta llegar a la ejecución de las 11:50h, momento a partir del cual se ve claramente como los valores rojo y azul bajan a los valores normales anteriores al incremento de spam recibido.

También se puede apreciar que a partir de ese momento la cantidad de e-mails rechazados por el **STS-MAILSAFE MILTER** (línea de color verde) se incrementa. Esto ha sido debido a que en la ejecución módulo de análisis de logs de las 11:50h, la heurística antispam que hemos explicado hace un momento le sirvió para identificar que desde una IP se estaba mandando demasiado spam (se superó el umbral de n mensajes spam por lapso de tiempo), motivo por el cual dicha IP fue añadida a la base de datos de lista negra para que fueran rechazadas las conexiones desde la misma.

