centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 681A21

IMPLEMENTACIÓN DE SEGURIDAD EN POSTFIX SOBRE RED HAT 8



SEPTIEMBRE 2021

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES

Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2021
NIPO: 083-21-163-3

Fecha de Edición: septiembre de 2021
Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD
El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL
Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN)

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

septiembre de 2021



Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL 5
2. INTRODUCCIÓN 5
3. OBJETO 6
4. ALCANCE 6
5. DESCRIPCIÓN DEL USO DE ESTA GUÍA 7
5.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA 8
5.2 ESTRUCTURA DE LA GUÍA 10
6. ARQUITECTURA Y SEGURIDAD EN POSTFIX 10
6.1 PARTES DE UN MENSAJE DE CORREO USADOS POR POSTFIX 11
6.2 REGISTROS DNS EN CORREOS ELECTRONICOS 12
6.3 FUNCIONAMIENTO INTERNO DE POSTFIX 12
6.3.1 PROCESO DE RECEPCIÓN DE UN MAIL EN POSTFIX 14
6.3.2 PROCESO DE ENTREGA DE UN MAIL EN POSTFIX 15
6.3.3 AGENTE DE ENTREGA MAILDROP 17
6.3.4 POSTFIX BACKEND 17
6.3.5 COMANDOS DE POSTFIX 22
6.4 CONFIGURACIÓN INICIAL 23
6.4.1 NOMBRE DE HOST 24
6.4.2 MÉTODO DE ENTREGA DIRECTO E INDIRECTO 25
6.4.3 REENVIO DE CORREOS (MAIL-RELAY) 25
6.4.4 POSTMASTER Y ALIASES 25
6.5 RECOMENDACIONES DE SEGURIDAD 26
6.5.1 GESTION DE REGISTROS Y AUDITORÍA EN POSTFIX 28
6.5.2 EJECUCIÓN DE PROCESOS DE DEMONIO POSTFIX CHROOT 29
6.5.3 ANTI-SPAM SPAMASSASSIN 29
6.5.4 CERTIFICADOS Y PROTOCOLOS SSL/TLS 30
6.5.5 REGLAS IPTABLES Y FIREWALL 32
6.5.6 GNUPG2 S-MIME 32
6.5.7 BLOQUEO DE CORREOS ZOMBIS CON POSTSCREEN 33
6.5.8 SPF EN POSTFIX 34
6.5.9 DKIM EN POSTFIX 36

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. INTRODUCCIÓN

Este documento forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para entornos basados en los productos y sistemas operativos de Linux (CCN STIC 600), siendo de aplicación para la Administración pública en el cumplimiento del Esquema Nacional de Seguridad (ENS) y de obligado cumplimiento para los sistemas que manejen información clasificada nacional.

La serie CCN-STIC-600 se ha diseñado de manera incremental. Así que, dependiendo del sistema, se aplicarán consecutivamente varias de estas guías. Esta guía ha sido orientada para configuración segura de servidores de correo electrónico basados Postfix 3.3, las guías que deberán aplicarse son:

a) La presente guía.

Nota: Las guías que son de aplicación para entornos de red clasificada están pensadas y diseñadas para entornos de máxima seguridad donde no existirá conexión con redes no seguras como puede ser Internet.

3. OBJETO

El propósito de este documento consiste en proporcionar los procedimientos para la implementación, establecer la configuración y realizar tareas de administración maximizando las condiciones de seguridad del servidor de correo Postfix en un servidor independiente Red Hat 8.3 Linux.

La configuración que se aplica a través de la presente guía se ha diseñado para ser lo más restrictiva posible, minimizando la superficie de ataque y por lo tanto los riesgos que pudieran existir. En algunos casos y dependiendo de la funcionalidad requerida del servidor, podría ser necesario modificar la configuración, que aquí se plantea, para permitir que el equipo proporcione servicios adicionales.

No obstante, se tiene en consideración que los ámbitos de aplicación son muy variados y por lo tanto dependerán de su aplicación, las peculiaridades y funcionalidades de los servicios prestados por las diferentes organizaciones. Por lo tanto, las normas de seguridad se han generado definiendo unas pautas generales de seguridad que permitan el cumplimiento de los mínimos establecidos en el ENS y las condiciones de seguridad necesarias en un entorno clasificado.

Esta guía asume que el servidor de correo se va a implementar sobre un equipo con un sistema operativo Red Hat 8.3 Linux, donde se ha seguido el proceso de implantación definido en las guías CCN-STIC-600.

Cumpliendo con estos requisitos previos, puede iniciar la instalación del servidor de correo Postfix MTA en modo relé.

Así mismo, no se contempla en esta guía la instalación y configuración de un servidor DNS, un servidor de correo principal, ni la implementación de certificados emitidos por una CA oficial.

4. ALCANCE

Esta guía ha sido elaborada con el fin de proporcionar información específica y con objeto de asegurar un servidor Agente de Transporte de Correo (con siglas en inglés MTA) Postfix, instalado en español en su versión 3.3.1-12.el8_3.1. Se incluyen, además, operaciones básicas de administración y aquellas acciones que deban ser llevadas a cabo para el mantenimiento y el buen uso de la aplicación.

El escenario en el cual está basada la presente guía responde a las siguientes características:

a) En el caso de aplicación del ENS, en cualquiera de sus diferentes categorías de seguridad, se establecerá un escenario con servicios adicionales sobre el sistema operativo Red Hat 8.3 Linux, al cual le aplican los procesos definidos en las guías CCN-STIC series 600 y en función de las categorías de seguridad establecidas en el ENS para clientes Red Hat 8.3 Linux independientes.

b) En el caso de tratarse de un entorno de red clasificada, se contempla un escenario compuesto por servicios adicionales a Red Hat 8.3 Linux a los cuáles le aplican los diferentes procesos definidos en los apartados relativos a la configuración de Red Hat 8.3 Linux en redes clasificadas y definidos, así mismo, en las guías CCN-STIC series 600.

Este documento incluye:

a) **Funcionalidades de seguridad local adicionales.** Completa descripción de aquellas características y servicios que, no encontrándose definidos por defecto, agregan seguridad adicional a una infraestructura de Red Hat 8.3 Linux como servidor independiente donde se le va a implementar Postfix.

b) **Mecanismos para la implementación de la solución.** Se incorporan mecanismos para la implementación de la solución de forma automatizada.

c) **Mecanismos para la aplicación de configuraciones.** Se incorporan mecanismos para la implementación de forma automática de las configuraciones de seguridad susceptibles de ello.

d) **Guía paso a paso.** Va a permitir implantar y establecer las configuraciones de seguridad para la solución Postfix en servidores Red Hat 8.3 Linux independientes.

e) **Lista de comprobación.** Ayuda a verificar el grado de cumplimiento de un servidor con respecto a las condiciones de seguridad que se establecen en esta guía.

f) **Guía de administración.** Proporciona el método para realizar las tareas de administración más comunes en el entorno de seguridad establecido.

5. DESCRIPCIÓN DEL USO DE ESTA GUÍA

Para entender esta guía de seguridad, es conveniente explicar el proceso de securización que describe y los recursos que proporciona. Este proceso constará de los siguientes pasos:

a) Antes de comenzar a aplicar esta guía, se deberá tener en cuenta que, además de los requisitos de seguridad a cumplir para la instalación de Postfix, será necesario cumplir los requisitos de seguridad definidos para Red Hat 8.3 (1.0, además de ser necesario comprobar los requisitos de otros servicios y aplicaciones que se vayan a implementar posteriormente. En la mayoría de los productos y/o servicios se recomienda tener en distintos puntos de montaje para el sistema operativo y el resto de ficheros de configuración del servicio proporcionado.

b) Si el entorno en el que está aplicando seguridad pertenece a una red clasificada, se deberá realizar la aplicación de seguridad del sistema operativo Red Hat 8.3 (1.0) e instalar Postfix 3.3.1-12.el8_3.1. Para ello, será necesario aplicar las guías CCN-STIC series 600. A continuación, se deberá instalar y configurar Postfix 3.3.1-12.el8_3.1 sobre Red Hat 8.3 (1.0), tal y como se describe en la presente guía.

c) En aquellos sistemas que les sea de aplicación el ENS estas medidas deberán adaptarse a las necesidades de cada organización.

d) El procedimiento establecido en este documento asume que se está configurando un sistema a partir de un entorno limpio (formateado) en el caso de una red clasificada y un entorno ya en producción en el caso del ENS.

5.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA

Los contenidos de esta guía son de aplicación a equipos con Sistema Operativo Red Hat 8.3 Linux en castellano, con el objetivo de reducir la superficie de exposición a ataques posibles con una instalación por defecto, manteniendo los principios de máxima seguridad, mínima exposición y servicios y mínimos privilegios que emanan de la guía CCN-STIC-301. En el caso de llevar a cabo la aplicación de esta guía sobre un servidor MTA Postfix con una configuración de idioma diferente al castellano, es posible que deba incorporar nuevos recursos y/o realizar ciertas modificaciones sobre los recursos que se adjuntan con este documento para permitir la correcta aplicación y uso del documento.

Para los entornos de ENS se podrá utilizar la versión de Red Hat 8.3 Linux, con la opción de instalación que más se adapte a las necesidades de cada organización.

En un entorno de red donde se maneja información clasificada, la única versión autorizada del Sistema Operativo Red Hat-8.3-x86_64 con la opción de instalación “instalación mínima”.

Las imágenes LiveCD y LiveDVD contienen un sistema de archivos comprimido de arranque, creado por un conjunto de scripts personalizados utilizan un archivo de configuración kickstart. Estas imágenes en vivo también se pueden instalar en el disco duro, obteniendo así una instalación de Red Hat totalmente funcional. El conjunto de paquetes instalados de esa manera en un disco duro no se puede ajustar durante la instalación, ya que es una transferencia simple de la imagen existente en CD / DVD a un disco duro. Después de arrancar desde el disco duro, Yum puede usarse para agregar o eliminar paquetes.

Las imágenes MinimalCD contienen un mínimo de paquetes necesarios para una instalación funcional, sin comprometer la seguridad o la usabilidad de la red. Estas imágenes mínimas usan el instalador estándar de Red Hat con todas sus características regulares menos la selección de paquetes. Yum se puede usar después de completar la instalación para agregar o eliminar paquetes.

La guía ha sido desarrollada y probada en entorno de uso de servicios Linux con la versión de Red Hat-8.3-x86_64.

La presente guía de seguridad ha sido elaborada mediante un laboratorio basado en una plataforma de virtualización tipo Hyper-V sobre Windows Server 2012 R2 Datacenter con las siguientes características técnicas:

a) Servidor Dell PowerEdge™ T320:

   i. Intel Pentium Xeon CPU ES 2430 2.20GHz.

   ii. HDD 1 TB.

   iii. 64 GB de RAM.

   iv. Interfaz de Red 1 Gbit/s.

No se puede garantizar el correcto funcionamiento de las configuraciones e implementaciones aplicadas mediante esta guía de seguridad si se hace uso de hardware que no cumpla con los requisitos de mínimos de Red Hat 8 Linux. Esto quiere decir que se requieren equipos con procesadores Intel o AMD de 64 o 32 bits (x64 o i386), con más de 1 GB de memoria RAM ambas versiones.

Se aconseja, no obstante, por seguridad y rendimiento, la implementación de versiones de 64 bits frente a las de 32 bits.

Nota: Puede comprobar los requisitos del sistema de Red Hat en el siguiente enlace https://access.redhat.com/articles/rhel-limits

Para garantizar la seguridad y funcionalidad de los servidores, deberán instalarse las actualizaciones de seguridad disponibles y recomendadas por el fabricante. Se deberá tener en cuenta la implementación de las actualizaciones tanto para el sistema operativo como para los diferentes servicios instalados, como el propio paquete de Postfix.

Dependiendo de la naturaleza de las distintas actualizaciones, el lector podrá encontrarse con algunas variaciones respecto a lo descrito en esta guía.

Las actualizaciones recomendadas por el fabricante están disponibles a través del servicio “yum update --security “. Las actualizaciones por lo general están disponibles en los servidores espejo (servidores que replican los propios de RED-HAT), en las siguientes 72 horas después de su publicación por el equipo de RED-HAT. Normalmente estos paquetes están disponibles en 24 horas, no obstante, hay que tener presente que determinadas actualizaciones, por su criticidad, pueden ser liberadas en cualquier momento. Se deberá tener en cuenta la implementación de las actualizaciones tanto para el sistema operativo como para los diferentes servicios instalados. Deberá tener en consideración RED-HAT ofrece diferentes tiempos de implementación de actualizaciones. En líneas posteriores de la presente guía se tratarán las consideraciones oportunas. Postfix al tratarse de una herramienta incluida en el propio sistema, se recomienda actualizar en conjunto con el sistema operativo Red Hat, respetando las versiones recomendadas por Red Hat 8 Linux.

La presente guía ha sido desarrollada con el objetivo de dotar a las infraestructuras de la seguridad adecuada dependiendo del entorno sobre el que se aplique. Es posible que algunas de las funcionalidades esperadas hayan sido desactivadas y, por lo tanto, pueda ser necesario aplicar acciones adicionales para habilitar servicios, demonios o características deseadas.

El espíritu de estas guías no está dirigido a remplazar políticas consolidadas y probadas de las organizaciones sino a servir como línea base de seguridad. Esta línea deberá ser adaptada a las necesidades propias de cada organización.

5.2 ESTRUCTURA DE LA GUÍA

Esta guía dispone de una estructura que diferencia la implementación de un servidor de correo Postfix dependiendo del entorno sobre el que vaya a ser aplicado, así como una diferenciación de la versión a utilizar. La guía dispone de las siguientes configuraciones divididas en dos grandes anexos, los cuales se definen a continuación:

a) **Anexo A:** En este anexo se define la configuración necesaria para adaptar los sistemas Linux y paquetes Postfix versión 3.3.1-12.el8_3.1 a las necesidades requeridas por el Esquema Nacional de Seguridad (ENS) en sus diferentes niveles de clasificación.

b) **Anexo B:** En este anexo se define la configuración necesaria para adaptar los sistemas Linux y paquetes Postfix versión 3.3.1-12.el8_3.1 a las necesidades requeridas en los entornos clasificados.

Cabe remarcar que en sus respectivos anexos se dotara de la información necesaria y concreta para cada tipo de implementación.

6. ARQUITECTURA Y SEGURIDAD EN POSTFIX

Postfix es un servidor de correo (MTA) de software libre y código abierto cuya principal característica es su fiabilidad en el envío y recepción de mensajes de correo electrónico. Postfix fue desarrollado principalmente con la finalidad de sustituir a otras soluciones MTA que presentaban vulnerabilidades conocidas. Así mismo, además de eliminar fallos de seguridad y mitigar vulnerabilidades, su aparición supuso también una disminución de la complejidad de configuración presente en dichas soluciones anteriores.

Postfix proporciona, en gran medida, confiabilidad y capacidad. Según la documentación oficial, Postfix, en arquitecturas de hardware con bajos recursos, podría recibir y entregar hasta un millón de mensajes al día. Esta confiabilidad y alto rendimiento vienen proporcionados por la detección automática de problemas como el agotamiento de la memoria o el espacio en disco. Así mismo, utiliza técnicas que limitan el número de nuevos procesos y accesos al sistema de archivos para el procesamiento de mensajes.

En lo que a seguridad se refiere, Postfix asume, de manera implícita, que se ejecuta en un entorno hostil y emplea múltiples capas de defensa utilizando el concepto de menor privilegio. Al estar compuesto de diferentes programas y subsistemas, cada elemento puede ser configurado de forma independiente, pudiendo establecer unos criterios de seguridad mucho más granulares y adecuados a cada entorno, incluyendo sistemas que pudieran manejar información clasificada o reservada.

Nota: Puede consultar los detalles y características del producto en la siguiente URL: http://www.postfix.org/start.html

Postfix utiliza una arquitectura tradicional tipo cliente-servidor. Un mensaje de correo electrónico se crea utilizando un programa cliente de correo, también conocido como MUA (Mail User Agent o Agente de Usuario de Correo). Este programa, envía el mensaje de correo electrónico al servidor de correo, el cual también se conoce como MTA o Mail Transport Agent (en español Agente de Transporte de Correo).

Posteriormente, el MTA, entrega el correo electrónico a otro componente del sistema denominado MDA (Mail Delivery Agent o Agente de Entrega de Correo), que es el encargado de entregar los correos electrónicos a los buzones de sus usuarios a través de su agente de usuario de correo. El MAA (Mail Access Agent o Agente de Acceso de Correo), así mismo, es el encargado de la interacción entre el servidor de correo electrónico y agente de usuario de correo.

La interacción entre los servidores de agentes de transporte de correo se realiza a través del protocolo SMTP (Simple Mail Transfer Protocol) con la ayuda de un servidor de traducción de nombre o DNS.

El acceso de los agentes de usuarios de correo a los buzones de correo electrónico se puede realizar a través de los protocolos tales como POP (Post Office Protocol), IMAP (Internet Message Access Protocol) o SMTP (Simple Mail Transfer Protocol), según se utilice un cliente pesado, un navegador o una consola de comandos SHELL.

6.1 PARTES DE UN MENSAJE DE CORREO USADOS POR POSTFIX

A continuación, se definen los componentes principales que contiene un mensaje:

a) **Encabezado del Mensaje**. En un correo electrónico el encabezado del mensaje es la parte más importante en el proceso de entrega. compone de etiquetas especiales tales como “From”, “Date”; “To” o “Bcc”, estas etiquetas almacenan información relativa a remitente, fecha de entrega, destinatario o aquellos usuarios que están en copia del mensaje.

b) **Cuerpo del mensaje**. Es la parte del correo electrónico más importante desde el punto de vista del usuario ya que contiene el mensaje que se quiere trasmitir. Dependiendo del cliente de correo o el protocolo utilizado para el envío del mensaje, el cuerpo del mensaje puede contener únicamente texto plano o puede tener diversos formatos de contenidos multimedia, como podrían ser texto enriquecido, video, imagen, etc.

c) **Encapsulamiento del mensaje**. Describe quien es el remitente del mensaje, para quien va dirigido y cómo debe de ser enviado. Esta parte del mensaje está más orientada al administrador del sistema, por su utilidad a la hora de detectar problemas en la comunicación entre servidores de correo y problemáticas en un nivel más bajo desde el punto de vista de las comunicaciones en un entorno de red, siendo el mismo encapsulamiento transparente para el usuario.

   Así mismo el estudio del encapsulamiento del mensaje permite detectar uso fraudulento del sistema de mensajería del correo electrónico con ataques de suplantación de identidad, envíos masivos de correos o propagación de código malicioso.

6.2 REGISTROS DNS EN CORREOS ELECTRONICOS

Un servidor DNS (Domain Name Server) es un servidor de traducción de nombres, es decir, su funcionalidad radica en traducir las direcciones IP's de redes TCP/IP en nombres descriptivos para identificar los diferentes elementos de los que se componen la red.

Uno de los aspectos básicos del correo electrónico es la configuración de DNS. Para poder enviar un correo electrónico, sobre todo si el destinatario es un elemento ajeno a nuestra red y por tanto la información va a viajar por una red externa. Postfix debe tener acceso confiable a un servidor de DNS para resolver nombres de aquellos elementos que intervienen en la ruta que ha de seguir el correo electrónico para establecer la comunicación. Para recibir correo, los dominios deben estar correctamente configurados permitiendo así a otros servidores de correo contactar con el servidor de Postfix.

Los registros DNS contienen información sobre la resolución y/o traducción de los datos, resolución de nombre y de direcciones IP, necesarios de consulta sobre un dominio.

Existen diferentes tipos de Registros DNS:

a) **Registros HOST (A) o (AAAA).** Son los registros que asocian un nombre o host a una dirección IP. Si estos registros son para IPv4 son registros tipo "A". Si estos registros son para IPv6 son denominados tipo "AAAA".

b) **Registros CNAME.** Son registros que se usan para especificar varios nombres o "alias" para un mismo servidor o elemento de red. Mediante los registros CNAME, se deben especificar los Mail Exchanger Record (MX) para cada dominio.

c) **Registros MX.** El registro de intercambio de correo (MX), es un recurso DNS que indica a los agentes de transporte de correo como deben ser encaminado los correos electrónicos. Los registros MX apuntan a los agentes de transporte de correo a los cuales envían un correo electrónico, y establece el orden de prioridad en el cual deben de recibirlo.

d) **PTR.** Es la resolución inversa de los registros host (A) de un DNS. Los registros PTR deben contener información de las IP´s del CNAME.

6.3 FUNCIONAMIENTO INTERNO DE POSTFIX

Postfix está formado por un conjunto de programas independientes de menor tamaño, cada uno de los cuales realiza una tarea específica. Esta modularización facilita la seguridad, la estabilidad y la flexibilidad del sistema.

Los diferentes módulos de los que se puede componer el ecosistema de Postfix, nos permiten disponer desde un agente de transporte de correo sencillo y liviano capaz de operar con unos requisitos mínimos de rendimiento o hasta llegar a disponer de un sistema de correo tan complejo como cualquier solución de correo del mercado.

A continuación, se enumeran los componentes o módulos que se contemplan en la instalación de esta guía:

a) **Amavis.** Es un filtro de contenido de código abierto para el correo electrónico que implementa la transferencia de mensajes de correo electrónico, la decodificación, algunos procesamientos, comprobaciones, y la interfaz con filtros de contenido externo para proporcionar protección contra el correo no deseado, virus y otros malwares.

b) **ClamAV.** Es un software antivirus open source (de licencia GPL) para las plataformas Windows, GNU/Linux, BSD, Solaris, Mac OS X y otros sistemas operativos semejantes a Unix.

c) **SpamAssassin.** Apache SpamAssassin es la plataforma antispam Open Source (fuentes abiertas) que ofrece a los administradores del sistema un filtro para clasificar el correo electrónico y bloquear el spam (correo electrónico masivo no solicitado).

d) **GNUPG2.** Es una implementación completa y gratuita del estándar OpenPGP. Permite cifrar y firmar sus datos y comunicaciones; Cuenta con un versátil sistema de administración de claves, junto con módulos de acceso para todo tipo de directorios de claves públicas.

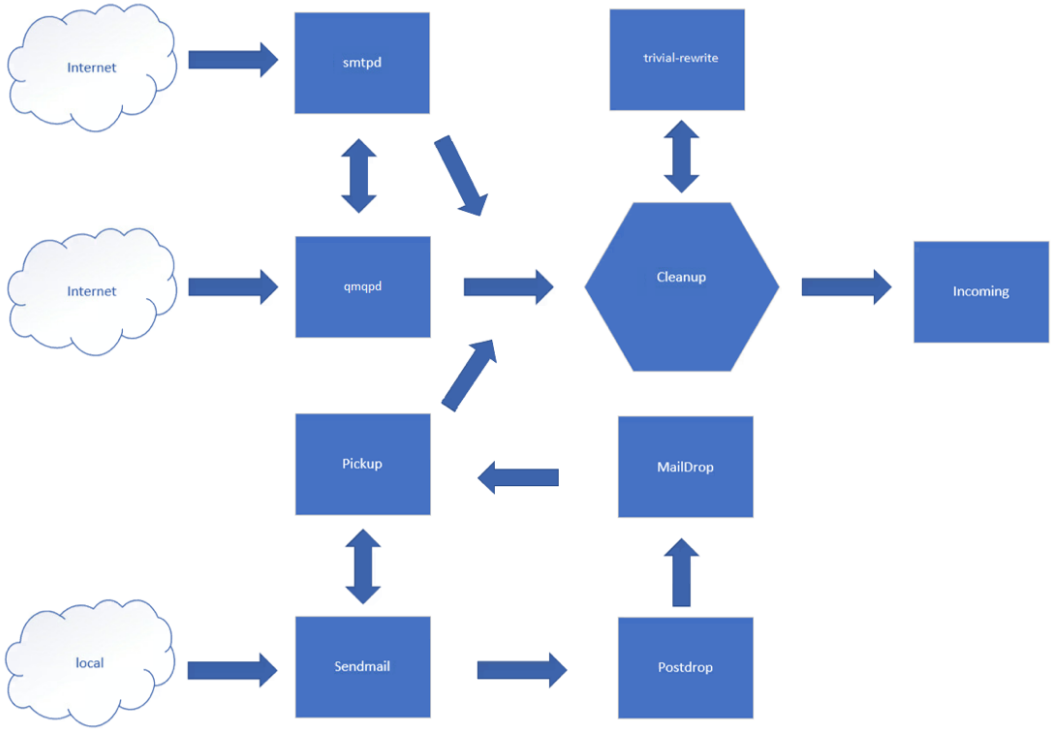
e) **OpenSSL.** Es un proyecto de software libre basado en SSLeay. Consiste en un robusto paquete de herramientas de administración y bibliotecas relacionadas con la criptografía, que suministran funciones criptográficas a otros paquetes como OpenSSH y navegadores web (para acceso seguro a sitios HTTPS).

f) **SPF.** Convenio de Remitentes (Sender Policy Framework) es una protección contra la falsificación de direcciones en el envío de correo electrónico. Identifica, a través de los registros de nombres de dominio (DNS), los servidores de correo SMTP autorizados para el transporte de mensajes. Este convenio busca ayudar a disminuir abusos como el spam.

g) **OpenDkim.** Domain Keys Identified Mail (DKIM) combina varios métodos anti-phishing y antispam existentes para mejorar la calidad de la clasificación e identificación del correo electrónico legítimo. En lugar de la dirección IP tradicional, para determinar el remitente del mensaje, DKIM agrega una firma digital asociada con el nombre de dominio de la organización.

6.3.1 PROCESO DE RECEPCIÓN DE UN MAIL EN POSTFIX

La siguiente figura muestra los principales procesos que están involucrados en todo el proceso de recepción un correo entrante. A continuación de la imagen se detalla la interactuación de los diferentes elementos desde la recepción del correo, siendo la fuente de origen local o externa, hasta la entrega al destinatario.



El correo de red, procedente de **Internet** o de una red externa, ingresa a Postfix a través de los servicios **smtpd** o **qmqpd**. Estos servicios eliminan el encapsulado del protocolo SMTP o QMQP, realizan algunas comprobaciones de seguridad y entregan el remitente, los destinatarios y el contenido del mensaje al servidor de limpieza (**cleanup**). El servidor smtpd puede configurarse para bloquear correo no deseado.

Los envíos recibidos desde una fuente **local** se reciben con el comando de compatibilidad Postfix **sendmail**, y a través del comando **postdrop** se ponen en cola de **maildrop**. Este proceso funciona incluso cuando el sistema de correo Postfix no se está ejecutando. El servidor de recogida local (**pickup**) recoge los envíos locales, aplica algunas comprobaciones de seguridad y entrega el remitente, los destinatarios y el contenido del mensaje al servidor de limpieza (**cleanup**).

El correo de las fuentes internas se entrega directamente al servidor de limpieza (**cleanup**). Las fuentes internas son aquellos servicios o procesos locales del propio servidor que comunican mediante correo electrónico un estado, configuración o alerta.

Un ejemplo de esto sería un mensaje informando que se ha sobrepasado la cuota permitida en un medio de almacenamiento determinado. Estas fuentes no se muestran en la figura e incluyen:

a) El correo que reenvía el agente de entrega local.

b) Los mensajes que el servidor "bounce" devuelve al remitente.

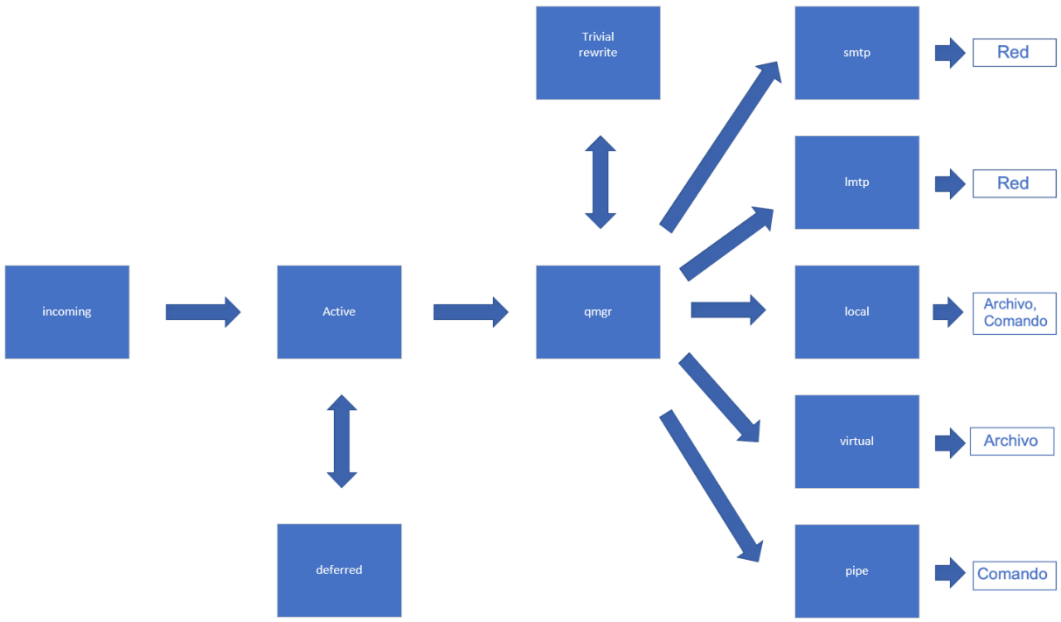
c) Notificaciones de Postmaster sobre problemas con Postfix.

El servidor de limpieza (**cleanup**) implementa la etapa de procesamiento final antes de que el correo se ponga en cola. Agrega los encabezados, y transforma las direcciones. Opcionalmente, el servidor de limpieza puede configurarse para realizar una inspección de contenido ligero con expresiones regulares. El servidor de limpieza coloca el resultado como un solo archivo en la cola entrante (**incoming**) y notifica al administrador de colas la llegada de correo nuevo.

El demonio **trivial-rewrite** interpreta y resuelve direcciones de correo, por ejemplo, transforma una dirección incompleta (usuario), en la dirección completa o en una dirección equivalente (usuario@sudominio.es), evitando así que se rechacen correos.

6.3.2 PROCESO DE ENTREGA DE UN MAIL EN POSTFIX

Una vez que un mensaje llega a la cola entrante (**incoming**), el siguiente paso es entregarlo, al núcleo del sistema de postfix y finalmente a su destinatario. La figura muestra los componentes principales del aparato de entrega de correo Postfix.



El administrador de colas (el proceso del servidor **qmgr** en la figura) es el núcleo de la entrega de correo de Postfix. Se pone en contacto con los agentes de entrega **smtp**, **lmtp**, **local**, **virtual** o **pipe**, y envía una solicitud de entrega para uno o más destinatarios. Los agentes de entrega de descarte y error son especiales: descartan o rechazan todo el correo y no se muestran en la figura anterior.

El gestor de colas separa los mensajes entre las colas activas (**active**) y diferidas (**deferred**). Mientras que en la cola activa se ubicarán los mensajes que pueden ser entregados de manera inmediata, en la cola diferida, se ubicarán aquellos mensajes de los cuales no es posible su entrega en el momento, por diversos motivos (por ejemplo, un equipo fuera de servicio o apagado). De este modo se libera la carga todo el proceso de entrega de correos y por consiguiente se optimiza su fluidez y eficacia.

El servidor **trivial-rewrite** resuelve cada dirección de destinatario según su clase de dirección local o remota. El servidor trivial-rewrite consulta los destinatarios cuya dirección ha cambiado; el correo para dichos destinatarios se devuelve al remitente con un breve mensaje explicativo indicando, el motivo del rechazo del mensaje.

El cliente smtp busca una lista de servidores de intercambio de correo para el equipo de destino, ordena la lista por preferencia y prueba cada servidor por turno hasta que encuentra un servidor que responda. Seguidamente encapsula el contenido del remitente, el destinatario y el mensaje según lo requiere el protocolo SMTP.

El cliente LMTP emplea un protocolo similar a SMTP que está optimizado para la entrega a servidores de buzones de correo. La ventaja de esta configuración es que una máquina Postfix puede alimentar múltiples servidores de buzones a través de LMTP. También es aplicable al proceso contrario, un servidor de buzones alimentado a través de LMTP por múltiples máquinas.

El agente de entrega local de Postfix es compatible con los buzones de correo de estilo UNIX, los archivos de “maildir” compatibles con “qmail”, las bases de datos de alias de todo el sistema de estilo Sendmail y los archivos forward por usuario de estilo Sendmail. Se pueden ejecutar múltiples agentes de entrega local en paralelo a diferentes agentes de transporte de correo compatibles, pero si las entregas en paralelo se realizan al mismo usuario, éstas generalmente son limitadas.

El agente de entrega local tiene enlaces para formas alternativas de entrega de mensajes en ámbito local, puede configurarse para entregar los archivos del buzón en los directorios de inicio del usuario, así mismo puede ser configurado para delegar la entrega del buzón a un comando externo como “procmail”, o puede delegar la entrega a un agente de Postfix diferente.

El agente de entrega virtual es un agente básico que se encarga de la entrega del correo a buzones de estilo UNIX o archivos maildir de estilo qmail únicamente. Éste puede repartir el correo para múltiples dominios, lo que lo hace especialmente adecuado para alojar muchos dominios pequeños en una sola máquina.

El correo electrónico **pipe** es la interfaz de salida a otros sistemas de procesamiento de correo (el comando postfix **sendmail** es la interfaz de entrada). La interfaz es compatible con UNIX: proporciona información en la línea de comandos y en el flujo de entrada estándar, y espera un código de estado de salida del proceso.

6.3.3 AGENTE DE ENTREGA MAILDROP

Los mensajes que se enviaron a través del comando **sendmail** Postfix pero que aún no han sido introducidos en la cola principal a través del servicio **pickup**, esperan el procesamiento en la cola "maildrop". Los mensajes se pueden agregar a dicha cola incluso cuando el sistema Postfix no se está ejecutando. Los mensajes se procesarán por Postfix cuando el servicio esté activo.

Se describen a continuación varias opciones para conectar el agente de entrega maildrop:

a) **Entrega directa sin el agente de entrega local**. Postfix puede configurarse para entregar correo directamente a maildrop sin usar, para ello, el agente de entrega local como intermediario. Esto significa que no obtiene la expansión de los alias locales, por lo que no realizaría consultas al fichero de aliases. Por lo general, este método se emplearía en dominios alojados con destinatarios que no tienen directorios de inicio de UNIX.

b) **Entrega indirecta a través del agente de entrega local**. Postfix puede ser configurado para entregar correo a maildrop a través del agente de entrega local. Este método es, en cierta medida, menos eficiente que el método de entrega directa descrito en el punto anterior, pero le brinda la comodidad de la expansión de alias y, por tanto, consulta el fichero de aliases. El uso de este método, normalmente, será apropiado para los dominios que se enumeran en “mydestination” y que tienen usuarios con una cuenta de sistema UNIX.

6.3.4 POSTFIX BACKEND

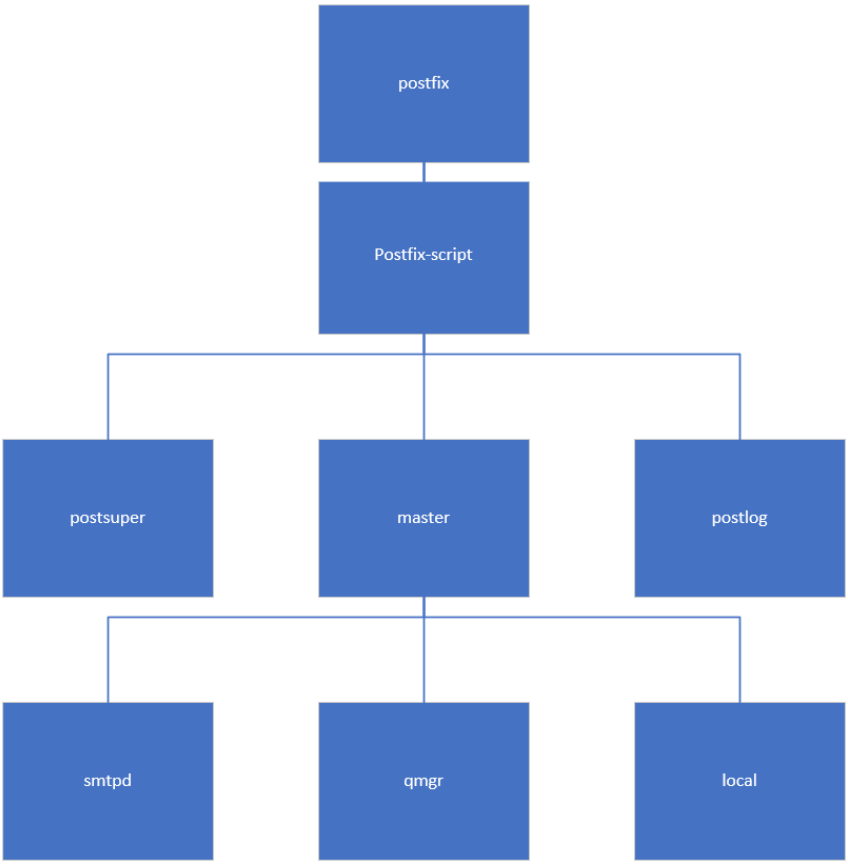
Las secciones anteriores dieron una descripción general de cómo los procesos del servidor Postfix envían y reciben correo. Estos procesos de servidor se basan en otros procesos que actúan a un nivel más bajo. El siguiente texto muestra cada uno de estos servicios en su propio contexto.

A continuación, se muestran varios de los procesos que actúan por debajo de los diferentes servicios principales de Postfix.

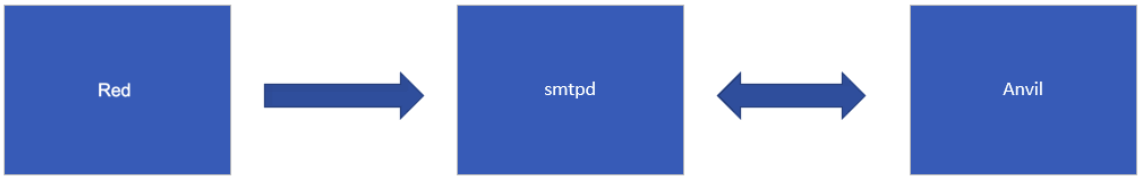
El servidor maestro residente (**master**) supervisa el correcto funcionamiento del sistema de correo de Postfix. Se inicia en el momento de arranque del sistema con el comando "**postfix start**" y continúa su ejecución hasta que el sistema se apaga. El servidor maestro es responsable de iniciar los procesos del servidor Postfix para recibir y entregar correo y de reiniciar los servidores que tengan una interrupción prematura debido a algún problema. El servidor maestro también es responsable de hacer cumplir los límites de conteo del proceso del servidor del modo en que se especifica en el archivo de configuración master.cf.

La siguiente imagen muestra la jerarquía del programa cuando se inicia Postfix. En el gráfico se muestra el orden de arranque y la jerarquía que emplean algunos de los diferentes procesos demonio de manejo de correo.

Cuando se da la orden de arranque de Postfix se ejecuta Postfix-Script, lo que desencadena el arranque de los procesos que serían el núcleo del sistema (master, postsuper, postlog). Una vez que master está en ejecución, éste a su vez, establece las conexiones por protocolos para posibilitar la recepción y el envío de los mensajes.

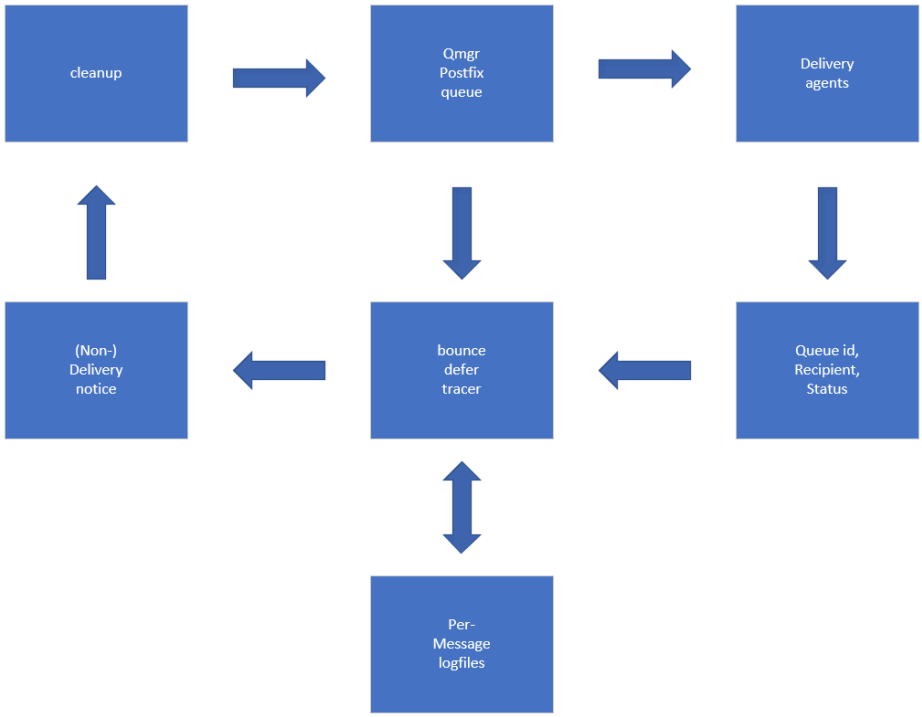


El servidor **anvil** implementa la conexión del cliente y la limitación de la tasa de solicitud para todos los servidores **smtpd**. **Anvil** controla la tasa de solicitud de conexiones simultaneas con la finalidad de evitar la pérdida del servicio por sobrecarga de tráfico o desbordamiento. El servicio **anvil** está disponible en la **versión 2.2** de **Postfix** y posteriores.

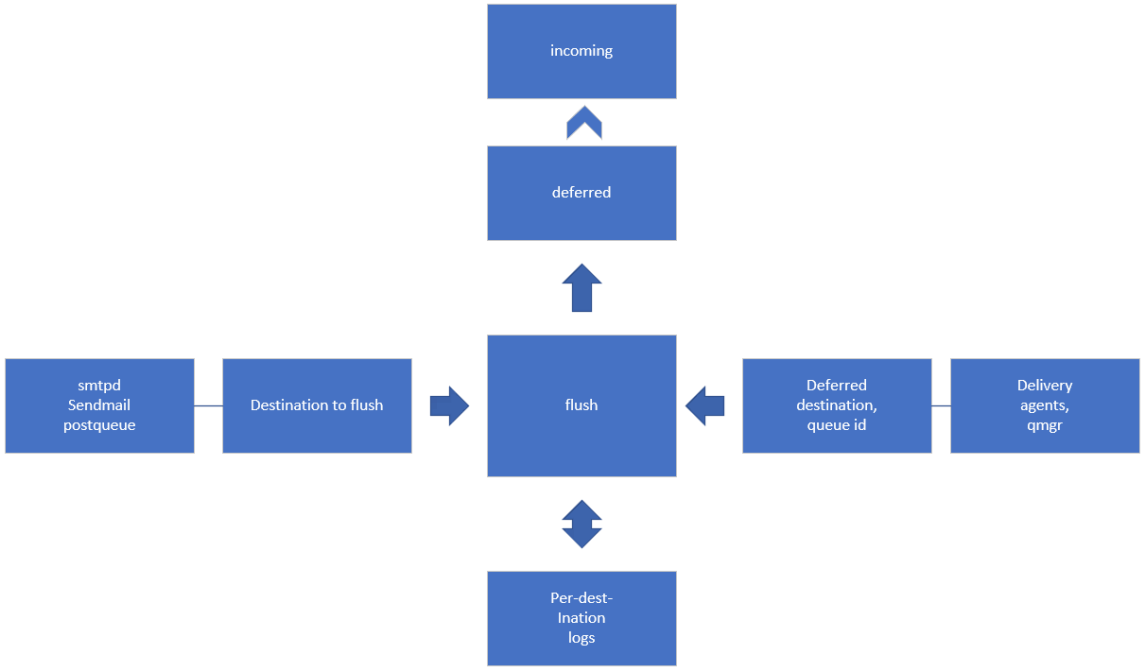


Los servicios **bounce**, **defer** y **tracer** mantienen sus propios árboles de directorios de cola mediante el uso de archivos de registro por mensaje. Postfix utiliza la información de dichos registros cuando envía notificaciones de estado de entrega ("fallido", "retrasado" o "exitoso") al remitente.

El servicio tracer también implementa la compatibilidad con los comandos "**sendmail -bv"** y "**sendmail -v"** de Postfix que producen informes sobre cómo Postfix entrega el correo, y está disponible con Postfix versión 2.1 y posteriores.



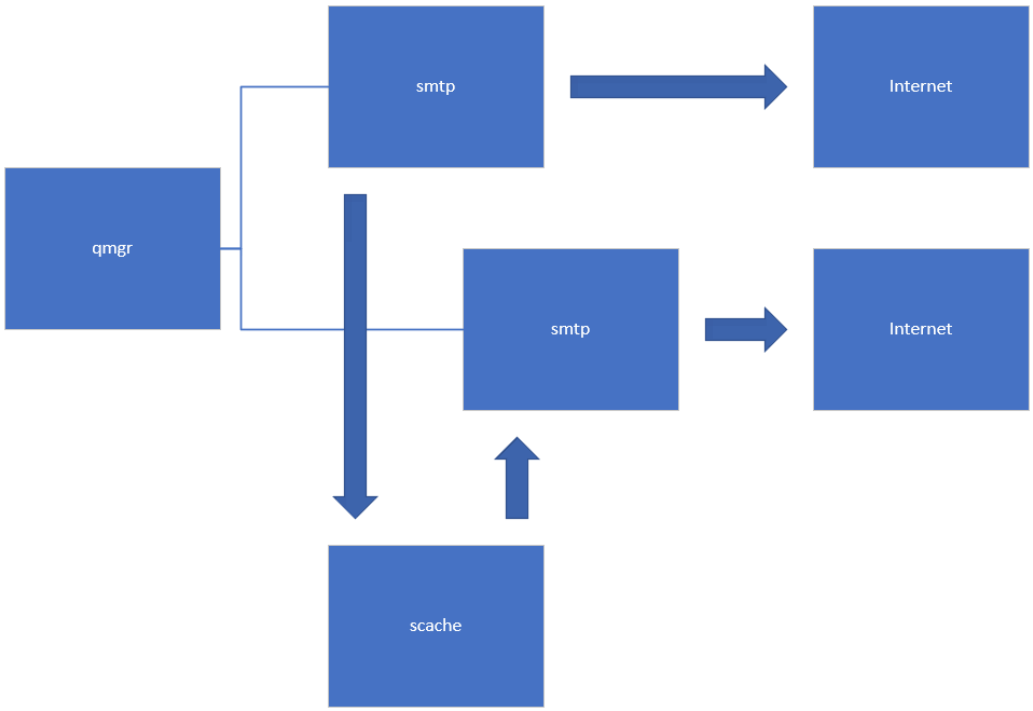
Los servidores de descarga (**flush** servers) mantienen registros por destino e implementan tanto ETRN como **sendmail -qR correo@dominio.es**. Esto mueve los archivos de cola seleccionados de la cola diferida (**Deferred**) a la cola entrante (**incoming**) y solicita su entrega. El servicio de descarga está disponible con Postfix versión 1.0 y posteriores.



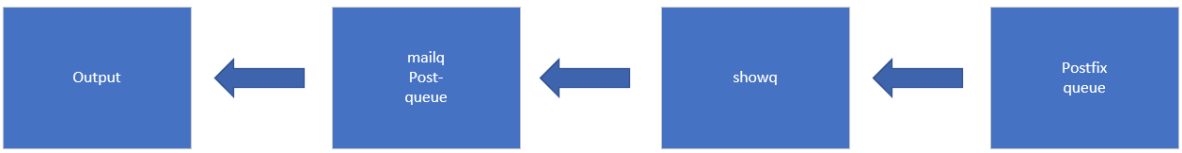
En caso de que la infraestructura haga uso de un servidor proxy, será necesario el empleo de servicios Proxymap. Los servidores Proxymap proporcionan un servicio de búsqueda de tablas de "solo lectura" y "lectura y escritura" para los procesos de Postfix. Esto supera las restricciones de chroot, reduce el número de búsquedas al compartir una tabla abierta entre varios procesos e implementa tablas de actualización única.

El servidor **scache** mantiene la caché de conexión para el cliente Postfix **smtp**. Cuando el almacenamiento en caché de la conexión está habilitado para los destinos seleccionados, el cliente **smtp** no se desconecta inmediatamente después de una transacción de correo, sino que proporciona la conexión al servidor de caché que mantiene dicha conexión abierta por un tiempo limitado. El cliente **smtp** continúa con alguna otra solicitud de entrega de correo. Mientras tanto, cualquier proceso **smtp** puede solicitar al servidor de scache esa conexión en caché y reutilizarla para la entrega de correo. Como medida de seguridad, Postfix limita la cantidad de veces que se puede reutilizar una conexión.

Cuando se entrega correo a un destino con múltiples servidores de correo, el almacenamiento en caché de la conexión puede ayudar a omitir un servidor que no responde, y así acelerar drásticamente la entrega. El almacenamiento en caché de la conexión SMTP está disponible en Postfix versión 2.2 y posteriores.



Los servidores **showq** listan el estado de la cola de Postfix (**Postfix queue**). Este es el servicio de listado de colas que hace el trabajo para los comandos **mailq** y **postqueue**.



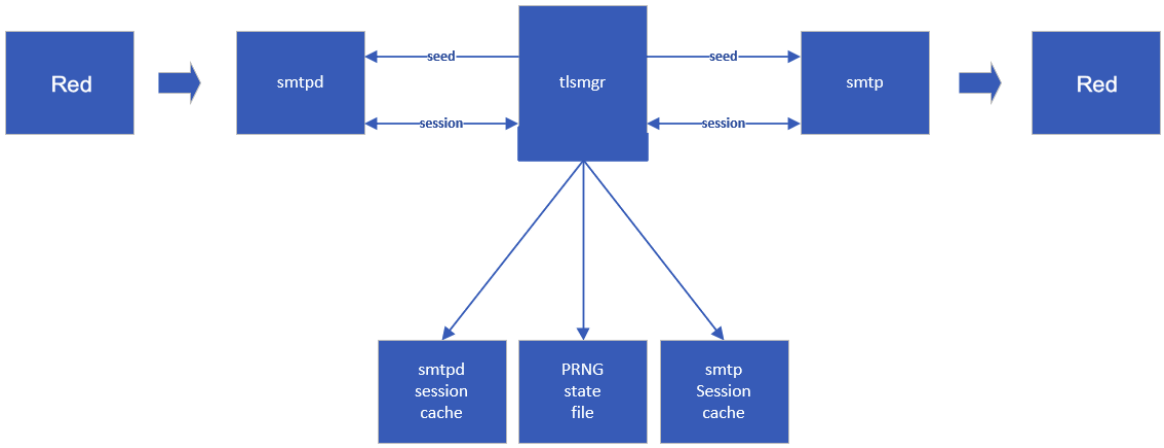
Los servidores spawn ejecutan comandos que no son Postfix, en respuesta con el cliente conectado a través de socket o FIFO a las corrientes de entrada, salida y error estándar del comando.

El servidor **tlsmgr** se ejecuta cuando TLS (Seguridad de la capa de transporte) está activada en el cliente **smtp** de Postfix o en el servidor **smtpd**. Este proceso tiene dos funciones:

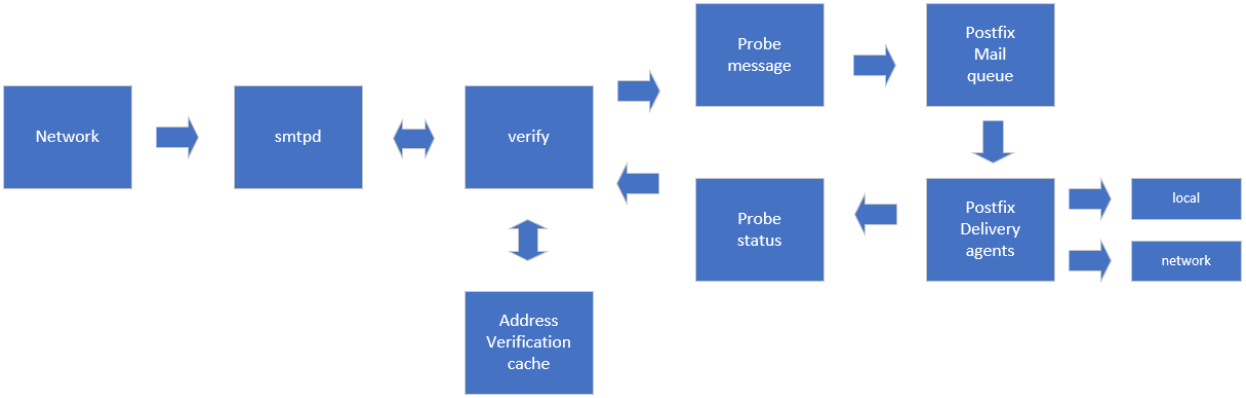
a) Mantener el generador de números pseudoaleatorios (**PRNG**) que se utiliza para inicializar los motores TLS en los procesos de cliente **smtp** o **smtpd** de Postfix. El estado de este **PRNG** se guarda periódicamente en un archivo y se lee cuando se inicia **tlsmgr**

b) Mantener las memorias caché del servidor **smtp** o **smtpd** opcionales con claves de sesión TLS. Las claves guardadas pueden mejorar el rendimiento al reducir la cantidad de operaciones al inicio de una sesión TLS.

La compatibilidad con TLS está disponible en Postfix versión 2.2 y posteriores.



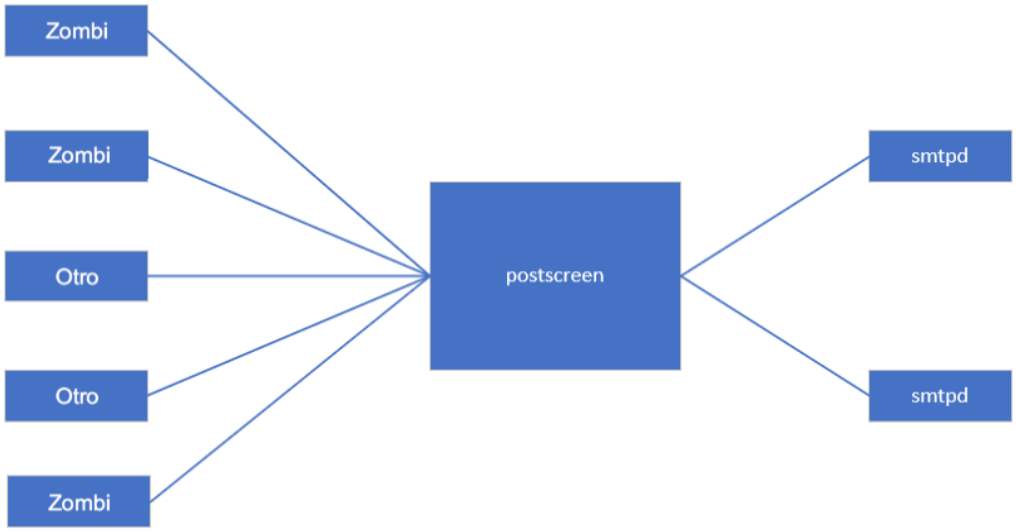
El servidor de verificación comprueba que la dirección del remitente o del destinatario se pueda entregar antes de que el servidor **smtpd** la acepte. El servidor de verificación (**verify**) consulta la caché con los resultados de la verificación de la dirección (**Address Verification Cache**). Si no se encuentra un resultado, el servidor de verificación inyecta un mensaje de prueba (**Probe Message**) en la cola de Postfix (**Postfix mail queue**) y procesa la actualización de estado (**Probe Status**) de un agente de entrega (**Postfix delivery agent**) o administrador de colas. El servicio de verificación está disponible con Postfix versión 2.1 y posteriores.



El servidor **postscreen** se puede colocar "al frente" de los procesos Postfix **smtpd**. Su propósito es aceptar conexiones de la red y decidir qué clientes SMTP pueden hablar con Postfix. Un porcentaje alto anual de todos los correos electrónicos podrían ser spam. Mientras postscreen mantiene alejados a los correos spam provenientes de servidores denominados servidores "**zombis"**, hay más procesos **smtpd** disponibles para clientes legítimos.

El servidor **postscreen** mantiene una lista blanca temporal para los clientes que pasan sus pruebas; Al permitir que los clientes de la lista blanca se salten las pruebas, postscreen minimiza su impacto en el tráfico de correo electrónico legítimo.

El servidor **postscreen** está disponible con Postfix 2.8 y versiones posteriores. Para mantener la implementación simple, **postscreen** delega las búsquedas de lista blanca / negra de DNS a los procesos del servidor dnsblog, y delega el cifrado / descifrado TLS a los procesos del servidor tlsproxy. Esta delegación es invisible para el cliente SMTP remoto y no se muestra en el diagrama a continuación.



6.3.5 COMANDOS DE POSTFIX

La descripción general de la arquitectura de Postfix termina con un resumen de las utilidades de línea de comandos para el uso diario del sistema de correo de Postfix. Además de los comandos **sendmail, mailq y newaliases** compatibles con Sendmail, el sistema Postfix viene con su propia colección de utilidades de línea de comandos.

Comando	Comportamiento
postfix	Controla el funcionamiento del sistema de correo. Es la interfaz para iniciar, detener y reiniciar el sistema de correo, así como para otras operaciones administrativas. Este comando está reservado al superusuario.
postalias	Mantiene bases de datos de tipo aliases de Postfix. Este es el programa que hace el trabajo para el comando "**newaliases"**.

Comando	Comportamiento
postcat	Muestra el contenido de los archivos de cola de Postfix. Esta es una utilidad preliminar limitada. Es probable que este programa sea reemplazado por algo más poderoso que también pueda editar los archivos de cola de Postfix.
postconf	Muestra o actualiza los parámetros de /etc/main.cf de Postfix y muestra información dependiente del sistema sobre los métodos de bloqueo de archivos compatibles y los tipos de tablas de búsqueda compatibles.
postdrop	Es la utilidad de publicación de correo que se ejecuta con el comando postfix "**sendmail"** para depositar el correo en el directorio de cola maildrop.
postkick	Hace que algunos canales de comunicación internos de Postfix estén disponibles para su uso en, por ejemplo, scripts de shell.
postlock	Proporciona un bloqueo de buzón compatible con Postfix para su uso en, por ejemplo, scripts de shell.
postlog	Proporciona un registro compatible con Postfix para los scripts de shell.
postmap	Mantiene las tablas de búsqueda de Postfix como canonical, virtual y otras.
postmulti	Repite el comando "**postfix start"**, etc. para cada instancia de Postfix, y admite la creación, eliminación, etc. de las instancias de Postfix.
postqueue	Es el comando privilegiado que se ejecuta con Postfix "**sendmail"** y "**mailq"** para vaciar o enumerar la cola de correo
postsuper	Mantiene la cola de Postfix. Elimina los archivos temporales antiguos y mueve los archivos de cola al directorio correcto después de un cambio en la profundidad de hashing de los directorios de cola. Este comando se ejecuta a la hora de inicio del sistema de correo y cuando se reinicia Postfix.

6.4 CONFIGURACIÓN INICIAL

Por defecto, los archivos de configuración de Postfix están situados en la ruta "/etc/postfix". Los dos archivos más importantes son **main.cf** y **master.cf**; estos archivos deben ser propiedad de root.

Postfix tiene varios parámetros de configuración que se controlan a través del archivo **main.cf**. Afortunadamente, todos los parámetros tienen valores predeterminados muy intuitivos. En muchos casos, se necesita configurar solo dos o tres parámetros antes de poder comenzar con el sistema de correo.

Nota: Los parámetros contemplados en todo el apartado de configuración inicial, se encuentran en el archivo "/etc /postfix/main.cf".

En /etc/postfix/main.cf deberá configurar un número mínimo de parámetros de configuración. Los parámetros de configuración de Postfix se asemejan a las variables del shell, con dos diferencias importantes: la primera es que Postfix no conoce las comillas como lo hace el shell UNIX.

El modo de especificar un parámetro de configuración será el siguiente:

/etc/postfix/main.cf:
parámetro = valor

Puede usar el parámetro $ antes de darle un valor (esa es la segunda diferencia principal con las variables de shell de UNIX). El lenguaje de configuración de Postfix no utiliza un valor de parámetro hasta que se necesita para su ejecución. Por tanto, al hacer uso de este símbolo "$", el valor se almacena en una variable para el documento (esta variable es un valor absoluto que puede ser invocado en más ocasiones a lo largo de dicho documento):

/etc/postfix/main.cf:
otro_parámetro = $ parámetro

Los procesos del demonio de Postfix se ejecutan en segundo plano y registran los problemas y la actividad normal en el demonio de rsyslog. En este apartado del documento se encuentran algunas cosas que deben ser tenidas en cuenta:

a) Si la máquina sobre la que aplica Postfix tiene requisitos de seguridad elevados, estos procesos deberán ser ejecutados (demonios) en una jaula chroot.

b) Si se ejecuta Postfix en una interfaz de red virtual, o si la máquina ejecuta otros correos en interfaces virtuales, los siguientes parámetros no podrán encontrarse vacíos (nulo):

   i. Nombre de host

   ii. Nombre de dominio

   iii. Direcciones de red

6.4.1 NOMBRE DE HOST

El parámetro myhostname especifica el nombre de dominio completo de la máquina que ejecuta el sistema Postfix. "$ myhostname" aparece como el valor predeterminado en muchos otros parámetros de configuración de Postfix.

De forma predeterminada, myhostname establece su valor en el nombre de la máquina local. Si el nombre de la máquina local no está en el formato de nombre de dominio completo o si se ejecuta Postfix en una interfaz virtual, será necesario especificar el nombre de dominio completo que debe usar el sistema de correo. Alternativamente, si se especifica mydomain, Postfix utilizará su valor para generar un valor predeterminado (FQDN) para el parámetro myhostname.

El parámetro mydomain especifica el dominio principal de "$ myhostname". De forma predeterminada, se deriva de "$ myhostname" eliminando la primera parte (a menos que el resultado sea un dominio de nivel superior). Por tanto, para este parámetro no sería necesario establecer un valor manualmente. Así mismo, si se especifica, de forma manual, mydomain, haciendo el proceso inverso, Postfix utilizará su valor para generar un valor predeterminado completo (FQDN) para el parámetro myhostname.

6.4.2 MÉTODO DE ENTREGA DIRECTO E INDIRECTO

Por defecto, Postfix intenta entregar el correo de forma directa. Dependiendo de las condiciones locales esto puede no ser posible. Por ejemplo, su sistema podría estar apagado. En esos casos, será necesario configurar Postfix para que realice las tareas de entrega de correo de forma indirecta, esta configuración deberá realizada a través de un host de retransmisión.

6.4.3 REENVIO DE CORREOS (MAIL-RELAY)

Postfix está configurado por defecto, para reenviar los correos autorizados por bloques a través de las redes autorizadas y hacia cualquier destino autorizado. Los bloques de redes autorizados vienen definidos por el valor “mynetworks”.

mynetworks_style = subnet (por defecto: subredes autorizadas)

El parámetro “relay_domains” hace referencia a qué dominios de destino se reenviarán los correos del sistema.

relay_domains = $mydestination (por defecto).

6.4.4 POSTMASTER Y ALIASES

El sistema Postfix reporta problemas del agente de transporte de correo al alias Postmaster, por defecto, el Postmaster está asignado al usuario administrador (root). Una medida de seguridad adicional para el sistema Postfix, es la asignación de la figura de Postmaster a un usuario administrador diferente a root.

La figura de Postmaster viene definida como el administrador del sistema de agente de transporte de correo de Postfix. Entre otros cometidos adquiere la figura del receptor de correos de error del propio sistema.

Debe configurar un alias de administrador de correo (debe ser un administrador del sistema), en la tabla de alias que redirige el correo. Se requiere que exista la dirección del administrador de correo, para que los usuarios puedan reportar problemas de entrega de correo. Mientras se realiza la actualización de la tabla de alias, será necesaria la redirección de correo a otro usuario con posibilidad de elevación de privilegios ya que en este momento el administrador de correo estaría no definido.

El sistema Postfix reporta de manera automatizada problemas a la figura administrativa del alias de Postmaster. Existe la posibilidad de que el número de informes y la información contenida en ellos, sea demasiado extensa y que mucha de la información no resulte relevante desde el punto de vista de la administración del sistema, por lo que este mecanismo de informes es configurable.

El valor predeterminado es informar solo los problemas graves (recursos, alteraciones de software) al administrador de correo. El significado de las diferentes clases de reportes es el siguiente:

a) **Rebotar**. Informa al administrador de correo, de correo "no entregable". O envía al administrador de correo una copia del correo que no se puede entregar, que se devuelve al remitente, o envía una transcripción de la sesión SMTP cuando Postfix rechazó el correo.

b) **Retrasar**. Informa al administrador del sistema, de correo retrasado. En este caso, el administrador recibe solo encabezados de mensajes. La notificación se envía a la dirección especificada con el parámetro de configuración **delay_notice_recipient** (el valor establecido como predeterminado es Postmaster).

c) **Política**. Informa al administrador de las solicitudes de los usuarios que se rechazaron debido a restricciones de la política (UCE). El administrador de correo recibe una transcripción de la sesión SMTP. La notificación se envía a la dirección especificada con el parámetro de configuración **error_notice_recipient** (el valor establecido como predeterminado es Postmaster).

d) **Recurso**. Informa al administrador de correo no entregado debido a problemas de recursos (por ejemplo, errores de escritura en archivos de cola). La notificación se envía a la dirección especificada con el parámetro de configuración **error_notice_recipient** (el valor establecido como predeterminado es Postmaster).

e) **Software**. Informa al administrador de correo no entregado debido a problemas de software. La notificación se envía a la dirección especificada con el parámetro de configuración **error_notice_recipient** (el valor establecido como predeterminado es Postmaster).

6.5 RECOMENDACIONES DE SEGURIDAD

Postfix utiliza archivos de base de datos para el control de acceso, la reescritura de direcciones y otros fines. Postfix admite diferentes bases de datos, tales como con Berkeley DB, LDARNGP o SQL.

Nota: Cuando se realice algún cambio en el archivo main.cf o master.cf, se deberá ejecutar el siguiente comando con privilegios de actualización para actualizar un sistema de correo en ejecución:
 # postfix reload

Atendiendo a la necesidad de aplicar medidas de refuerzo de seguridad en aquellos escenarios de gestión de correo electrónico con Postfix, a lo largo de esta guía, en sus diferentes Anexos, se identifican y establecen las directrices y condiciones necesarias para incrementar los niveles de seguridad según los criterios definidos en cada apartado.

Las medidas a adoptar se materializarán bien en la aplicación de plantillas de seguridad o bien en procedimientos de refuerzo. En este último caso, por ejemplo, para la segregación de roles, se detallarán procedimientos y condiciones que deberá aplicar un administrador de una organización para hacerlas efectivas.

Como norma general, se han identificado las siguientes recomendaciones y medidas de seguridad, las cuales son aplicables a Postfix sobre Red Hat 8, aunque también se puedan extender a otros sistemas operativos y MTA:

a) Aplicar un modelo de seguridad en profundidad en donde se incluyan todos los elementos que intervienen en el servicio de correo electrónico como son componentes de red, sistemas operativos, servicios y aplicaciones.

b) Habilitar únicamente los servicios necesarios para el transporte de correo electrónico.

c) Cifrar comunicaciones internas y externas de cualquier naturaleza y protocolo.

d) Implementar protocolos y algoritmos de cifrado robustos en todos los dominios y espacios de nombres SMTP, cuya comunicación incluya contenido potencialmente sensible.

e) Implementar y proporcionar a los usuarios mecanismos de cifrado y control de la información adicionales como S/MIME o PGP, especialmente en entornos clasificados de nivel alto.

f) Autenticar siempre usuarios y equipos antes de hacer uso de los servicios de correo electrónico, especialmente en aquellas comunicaciones de tipo retransmisión de mensajes.

g) Configurar mecanismos de defensa ante correo electrónico no deseado y código dañino.

h) Configurar directivas SPF y DKIM para proteger a la organización ante intentos de suplantación de identidad de usuarios o dominios.

i) Habilitar los registros de auditoría y acceso al servidor.

j) Implementar directivas de refuerzo de la seguridad en los servidores Red Hat 8 en donde esté instalado Postfix.

k) Implementar directivas de seguridad de Firewall.

l) Aplicar todas las actualizaciones disponibles por el fabricante tanto para el propio Postfix como para todos sus componentes y el sistema operativo.

m) Aplicar un control estricto de roles de usuarios que tienen permisos administrativos en Postfix, así como acceso a los registros de auditoría, colas de mensajes y servicios en general.

n) Instalar y configurar una solución antivirus desarrollada especialmente para Postfix, que permita detectar código dañino en el transporte.

Nota: En esta guía, se ha seleccionado el sistema operativo Red Hat 8 por considerarse suficientemente seguro para realizar funciones de sistema de correo electrónico MTA. En cualquier caso, muchas, si no todas, las medidas y recomendaciones presentadas anteriormente son aplicables a otras distribuciones de Linux, en las cuales se pueda instalar Postfix como servidor de correo electrónico.

6.5.1 GESTION DE REGISTROS Y AUDITORÍA EN POSTFIX

Los procesos del demonio de Postfix se ejecutan en segundo plano y registran los problemas y la actividad normal en el demonio de rsyslog. El proceso rsyslogd ordena los eventos por clase y gravedad, y los agrega a los archivos de registro. Las clases de registro, los niveles y los nombres de los archivos de registro se especifican en /etc/rsyslog.conf. Es necesario editar entradas en el archivo /etc/rsyslog.conf para errores de Postfix.

Tras aplicar los cambios al archivo rsyslog.conf, se deberá enviar una señal "SIGHUP" al proceso rsyslogd.

Nota: Muchas implementaciones de rsyslogd no crearán archivos. Será necesario crear archivos antes de reiniciar rsyslogd para la correcta configuración de los logs de Postfix.

Así mismo, será necesaria la ejecución periódica de la rotación de los registros de logs en rsyslog.

El comando "**postfix logrotate**" puede ser ejecutado de inmediato o a través de una tarea programada (**cronjob**), registrando todos los errores e informando de errores de salida estándar (stderr) si se ejecuta desde un terminal.

Postfix consta de una serie de programas demonio y programas no demonio, algunos de los cuales se utilizan para el envío de correo local y otros para la administración de Postfix.

La realización de la actividad de registro en los logs y la salida estándar de Postfix requiere hacer uso del servicio Postfix **postlogd**. Este demonio garantiza que cuando se registren diferentes logs de Postfix simultáneamente, estos no se mezclen entre sí.

Postfix es un agente de entrega de correo modularizado, que cuenta con multitud de módulos o programas que se pueden añadir al conjunto del sistema, de este modo es posible ampliar, modificar y complementar el comportamiento en conjunto de todo el sistema de correo. Cada módulo trabaja de manera independiente y para el conjunto de Postfix. Todo ello, a través de sus propios procesos y demonios.

Todos los programas de Postfix pueden iniciar sesión en rsyslog, pero no todos los programas tienen suficientes privilegios para usar los servicios de registro de Postfix. Muchos de estos programas que no son demonio no deben iniciar sesión en **stdout** (salida estándar) ya que eso dañaría su salida.

Los programas Postfix que no sean demonios, pueden registrar errores en rsyslogd antes de que hayan sido integrados en la configuración de Postfix con los parámetros definidos del archivo main.cf, y siendo integrados en el comportamiento en conjunto de Postfix.

Si Postfix está inactivo, los programas no demonio postfix, tales como **postsuper**, **postmulti** y **postlog** se registrarán directamente en el archivo de log **maillog**.

Otros programas de Postfix que no sean demonio nunca escribirán directamente en el maillog (también, el registro en **stdout** podría interferir con el funcionamiento de algunos de estos).

6.5.2 EJECUCIÓN DE PROCESOS DE DEMONIO POSTFIX CHROOT

El proceso de **chroot** en los sistemas operativos derivados de Unix, es una operación que invoca un proceso, cambiando para este y sus hijos el directorio raíz del sistema. Comúnmente, el entorno virtual creado por chroot a partir de la nueva raíz del sistema se conoce como "**jaula chroot**".

Los procesos demonio de Postfix se pueden configurar, a través del archivo /etc/postfix/master.cf, para que se ejecuten en una jaula chroot. Los procesos se ejecutan con un bajo privilegio fijo y con acceso al sistema de archivos limitado a los directorios de cola de Postfix (**/var/spool/postfix**). Esto proporciona una barrera contra ataques

Los demonios de Postfix pueden ejecutarse, al igual que sus servicios, en una jaula chroot, con la excepción de los demonios de Postfix que entregan el correo localmente y que ejecutan comandos que no son de Postfix.

Para obtener ciertos requisitos de seguridad se debe tener en consideración la aplicación de una jaula chroot a todos los demonios que comunican con procesos de red, como los procesos smtp y smtpd.

Los valores predeterminados de configuración de Postfix, especifican que ningún demonio se ejecute en una jaula chroot. Deberá habilitar la operación chroot, editando el archivo /etc/postfix/master.cf.

Será necesario tener en consideración que un demonio chroot resuelva todos los nombres de archivo relativos al directorio de cola de Postfix (/var/spool/postfix). Para que el uso de una jaula chroot sea exitoso, la mayoría de los sistemas UNIX requieren el ingreso de algunos archivos o nodos de dispositivos.

6.5.3 ANTI-SPAM SPAMASSASSIN

El spam, correo automático no deseado, se inició hace varios años con correos publicitarios molestos que, con el tiempo, se transformaron en una seria amenaza técnica, económica y social.

El spam bloquea los canales de comunicación y crea tráfico que genera inconvenientes tanto al proveedor como al propio usuario. Hay servidores de correo que reciben y procesan el spam. Estos servidores tienen que ser mantenidos por especialistas altamente remunerados. Por lo consiguiente hay una infraestructura de costos sustanciales de ejecución.

Si el spam llega a la bandeja de entrada, el destinatario tiene que eliminarlo manualmente. En caso de no disponer de ningún tipo de filtro que impida su entrada, una persona que lee 10-20 correos electrónicos por día, recibiría una gran cantidad de spam junto con su correspondencia. Esto se traduce en un promedio de varias horas por mes eliminando spam, en detrimento de un tiempo de trabajo productivo.

Una de las peores consecuencias de la eliminación manual de correo es perder por error un correo electrónico importante por tener que eliminar una gran cantidad de correo no deseado.

Apache SpamAssassin es la plataforma antispam Open Source (fuentes abiertas) que ofrece a los administradores del sistema un filtro para clasificar el correo electrónico y bloquear el spam (correo electrónico masivo no solicitado).

Esta herramienta utiliza un sólido marco de puntuación y complementos para integrar una amplia gama de pruebas de análisis estadístico y heurístico (el sistema es capaz de realizar tareas de autoaprendizaje para reconocer los mensajes que podrían ser considerados spam) avanzado en encabezados de correo electrónico y texto del cuerpo, incluyendo el análisis de texto, el filtrado bayesiano (este tipo de filtrado utiliza un teorema matemático para realizar dichos análisis), las listas de bloqueo de DNS y las bases de datos de filtrado colaborativo.

Apache SpamAssassin es un proyecto de Apache Software Foundation (ASF). Sus características principales son:

a) **Amplio espectro:** SpamAssassin utiliza una amplia variedad de pruebas locales y de red para identificar firmas de spam. Este hecho provoca que sea más difícil para los spammers (usuarios que generan contenido spam) identificar un aspecto en el que pueden elaborar sus mensajes de spam para eludir las medidas de seguridad.

b) **Software gratuito:** se distribuye bajo los mismos términos y condiciones que otros paquetes populares de software de código abierto, como el servidor web Apache.

c) **Fácil de extender:** las pruebas y la configuración de antispam se almacenan en texto sin formato, lo que facilita la configuración y la adición de nuevas reglas.

d) **Flexible:** SpamAssassin encapsula su lógica en una API abstracta para que pueda integrarse en cualquier lugar del flujo de correo electrónico. Las clases Mail SpamAssassin se pueden usar en una amplia variedad de sistemas de correo electrónico, incluyendo procmail, sendmail, **Postfix**, qmail, entre otros.

e) **Fácil configuración:** SpamAssassin requiere muy poca configuración; no es necesaria la aplicación de actualizaciones continuas con los detalles de sus cuentas de correo, membresías de listas de correo, etc. Una vez que esté clasificado, las políticas específicas del usuario y del sitio pueden aplicarse al correo no deseado. Las políticas pueden aplicarse a los servidores de correo, utilizando la propia aplicación de agente de correo del usuario.

6.5.4 CERTIFICADOS Y PROTOCOLOS SSL/TLS

SSL y TLS son protocolos criptográficos que proporcionan autenticación y cifrado de la información entre servidores, máquinas y aplicaciones que operan sobre una red.

SSL es el predecesor del TLS. Con los años, nuevas versiones de protocolos han sido desarrolladas para enfrentar las vulnerabilidades y para entregar cifrado y algoritmos más fuertes. SSL fue originalmente desarrollado por Netscape y fue introducido en 1995 con el SSL 2.0 (el 1.0 nunca fue lanzado al público). La Versión 2.0 fue rápidamente remplazada por el SSL 3.0 en 1996 después de que se comprobara la existencia de un gran número de vulnerabilidades que comprometían el protocolo. El TLS fue introducido en 1999 como una nueva versión del SSL y fue basada en SSL 3.0.

Nota: Versiones 2.0 y 3.0 son algunas veces nombradas como SSLv2 y SSLv3.

Tanto SSL 2.0 y SSL 3.0 han sido reemplazadas por otros protocolos. A lo largo de los años, se han detectado muchas vulnerabilidades derivadas del uso de protocolos SSL obsoletos. Por estas razones, se deberán deshabilitar SSL 2.0 y 3.0 en la configuración de los servidores, dejando habilitados los protocolos TLS únicamente.

Será necesario tener en consideración que certificados y protocolos no se refieren a lo mismo. Es importante hacer un inciso en que los certificados no dependen de los protocolos. En otras palabras, no es necesario usar certificados TLS en lugar de certificados SSL. En muchas ocasiones se tiende a usar la frase "certificado SSL/TLS", para ser más exactos se debe denominar "certificados para uso con SSL y TLS" ya que los protocolos son determinados por la configuración del servidor, y no por los certificados.

La Seguridad de la capa de transporte TLS (anteriormente llamada SSL) proporciona una autenticación basada en certificados y sesiones cifradas. Una sesión cifrada protege la información que se transmite mediante el correo SMTP o con la autenticación SASL.

La autenticación SASL se implementa por separado de Postfix. Por este motivo, la configuración de la autenticación SASL en el servidor SMTP implica dos pasos diferenciados:

a) Configuración de la implementación de SASL para ofrecer una lista de mecanismos adecuados para la autenticación y, dependiendo de la implementación de SASL utilizada, configuración de backends de autenticación, que verifiquen los datos de autenticación del cliente SMTP remoto, enfrentándolo al archivo de contraseñas del sistema o alguna otra base de datos.

b) Configuración del servidor SMTP de Postfix para habilitar la autenticación SASL y para autorizar a los clientes a retransmitir el correo o para controlar qué correos envían las direcciones que el cliente puede usar.

La autenticación exitosa en el servidor SMTP de Postfix requiere un marco de trabajo SASL funcional. Por lo tanto, la configuración de SASL siempre deberá ser un paso previo a la configuración de Postfix.

Actualmente, el servidor SMTP de Postfix admite las implementaciones Cyrus SASL y Dovecot SASL.

Nota: Las versiones actuales de Postfix tienen una arquitectura de complemento que puede admitir varias implementaciones SASL. Antes de la versión 2.3 de Postfix, Éste solo era compatible con Cyrus SASL. Para averiguar qué implementaciones de SASL se compilan en Postfix, use los siguientes comandos:
#postconf -a (compatibilidad con SASL en el servidor SMTP)
#postconf -A (compatibilidad con SASL en el cliente SMTP + LMTP)

Para utilizar TLS, el servidor SMTP de Postfix hará uso de un certificado y una clave privada. Ambos deben estar en formato **"PEM"**. La clave privada no debe estar cifrada, lo que significa que la clave debe ser accesible sin una contraseña. El certificado y la clave privada pueden estar en el mismo archivo, en cuyo caso el archivo del certificado debe ser propiedad de "root" y no ser legible por ningún otro usuario. Si la clave se almacena por separado, esta restricción de acceso se aplica solo al archivo de clave, y el archivo de certificado puede ser "legible para todo el mundo".

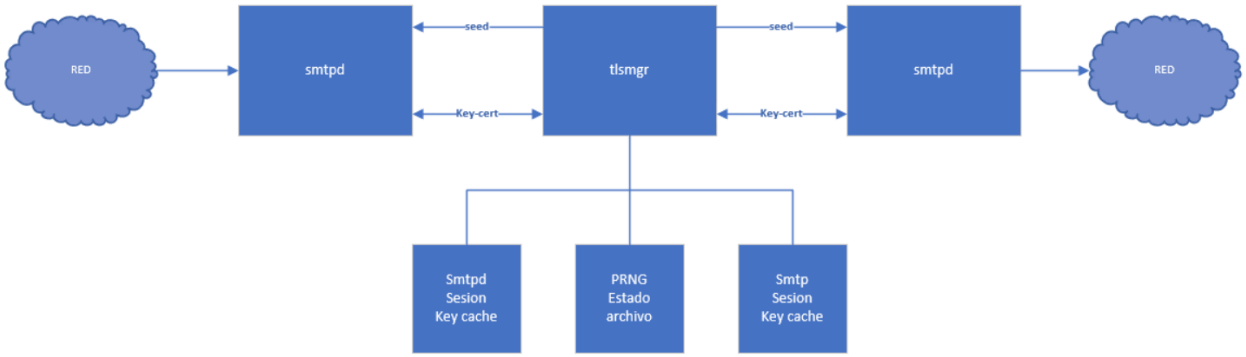
El siguiente diagrama muestra los elementos principales de la arquitectura TLS de Postfix y sus relaciones.

a) El servidor **smtpd** implementa el SMTP sobre el lado del servidor TLS.

b) El cliente **smtp** implementa el SMTP (y LMTP) en el lado del cliente TLS.

c) El servidor **tlsmgr** mantiene el generador de números pseudoaleatorios (PRNG) que genera los motores TLS en el servidor smtpd y los procesos cliente smtp, además mantiene los archivos de caché de claves de sesión TLS.

Nota: No se muestran en la figura el servidor tlsproxy ni el servidor postscreen. Estos utilizan TLS de la misma manera que smtpd.



6.5.5 REGLAS IPTABLES Y FIREWALL

La forma más sencilla de configurar Postfix en un host que se encuentra en una red tras un cortafuegos es establecer una redirección de todo el correo hacia un host que tenga la función de puerta de enlace y permitir que este host de correo se encargue del reenvío interno y externo. Otro enfoque sería enviar solamente correo externo al host que tiene una función de puerta de enlace y enviar correo el de intranet directamente a la red interna.

Para evitar tener que hacer uso de estas configuraciones, será necesario añadir las excepciones oportunas referentes a los puertos necesarios para el correcto funcionamiento de los protocolos y demonios de Postfix en el sistema de firewall o añadir las reglas pertinentes si su organización posee una configuración de IPTABLES. Estas configuraciones deberán ser adaptadas a las necesidades específicas de cada organización.

6.5.6 GNUPG2 S-MIME

GnuPG es una implementación completa y gratuita del estándar OpenPGP según lo define RFC4880 (también conocido como PGP). GnuPG permite el cifrado y la firma de los datos y comunicaciones; cuenta con un versátil sistema de administración de claves, junto con módulos de acceso para todo tipo de directorios de claves públicas. GnuPG, también conocido como GPG, es una herramienta de línea de comandos cuyas características permiten la integración con otras aplicaciones. GnuPG proporciona una gran cantidad de aplicaciones de frontend y bibliotecas, así como soporte para S / MIME y Secure Shell (ssh).

Desde su introducción en 1997, GnuPG es software libre, por lo que puede ser utilizado, modificado y distribuido libremente de acuerdo con los términos de la Licencia Pública General de GNU. El uso del cifrado ayuda a proteger la privacidad de remitentes y destinatarios que participan en el proceso de comunicación.

GnuPG cifra los mensajes usando pares de claves individuales asimétricas generadas por los usuarios. Las claves públicas pueden ser compartidas con otros usuarios de diversas maneras, un ejemplo de ello es depositándolas en los servidores de claves. Siempre deben ser compartidas cuidadosamente para prevenir falsas identidades por la corrupción de las claves públicas. También es posible añadir una firma digital criptográfica a un mensaje, de esta manera la totalidad del mensaje y el remitente pueden ser verificados en caso de que se desconfíe de una correspondencia en particular. GnuPG también soporta algoritmos de cifrado simétricos, por ejemplo, CASTS. GnuPG no usa algoritmos de software que están restringidos por patentes. En su lugar usa una serie de algoritmos no patentados como CAST5, Triple DES (3DES) y AES.

GnuPG es un software de cifrado híbrido que usa una combinación convencional de criptografía de claves simétricas para la rapidez y criptografía de intercambio de claves públicas para la fácil distribución de claves seguras, usando recipientes de claves públicas para el cifrado. Este modo de operación es parte del estándar OpenPGP y ha sido parte del PGP desde su primera versión. Por su manera de operar, permite mantener las comunicaciones en un alto nivel de seguridad, pero sin sacrificar el rendimiento en las comunicaciones. En un primer establecimiento, los dos elementos (remitente y destinatario) que participan en la comunicación, establecen la misma a través del intercambio de la parte pública de sus certificados asimétricos. Una vez establecido el túnel de comunicaciones, los cifrados de las mismas se realizarán a través de claves simétricas.

6.5.7 BLOQUEO DE CORREOS ZOMBIS CON POSTSCREEN

El demonio Postfix postscreen proporciona una protección adicional contra la sobrecarga del servidor de correo por correo no deseado. Un proceso postscreen maneja múltiples conexiones SMTP entrantes y decide qué clientes pueden comunicarse con un proceso del servidor SMTP Postfix. Al mantener alejados a los spambots, postscreen deja más procesos de servidor SMTP disponibles para clientes legítimos y evitando, de ese modo, la sobrecarga del servidor.

Postscreen no debe usarse en puertos SMTP que reciben correo de clientes finales (MUA). En una implementación habitual, postscreen maneja el servicio MX en el puerto TCP 25, mientras que los clientes MUA envían el correo a través del servicio de envío en el puerto TCP 587 que requiere la autenticación del cliente.

Así mismo, Postscreen mantiene una lista blanca temporal para los clientes que superan sus pruebas; Al permitir que los clientes de la lista blanca no vuelvan a realizar dichas pruebas, postscreen minimiza su impacto en el tráfico de correo electrónico legítimo.

Postscreen es parte de una defensa de múltiples capas:

a) Como primera capa, postscreen bloquea las conexiones de zombis y otros spambots que son responsables de la mayoría del spam generado. Este proceso se implementa como un elemento único para hacer que esta defensa sea lo más liviana posible para los recursos.

b) La segunda capa implementa verificaciones de acceso más complejas a nivel SMTP con servidores Postfix SMTP, demonios de políticas y aplicaciones Milter (filtrado de correo masivo no deseado).

c) La tercera capa realiza una inspección de contenido de partes del correo electrónico con las opciones header_checks y body_checks incorporadas de Postfix. Esto puede bloquear archivos adjuntos potencialmente peligrosos, como programas ejecutables, y gusanos o virus con firmas fáciles de reconocer.

d) La cuarta capa proporciona inspección de contenido pesado con filtros externos de contenido. Ejemplos típicos son las aplicaciones Amavisd-new, SpamAssassin y Milter.

La mayoría del correo electrónico spam, es enviado por zombis (malware en las computadoras de usuarios finales comprometidos). Sin una herramienta como postscreen, que mantenga alejados a los zombis, se estarían consumiendo la mayoría de los recursos impidiendo realizar las tareas que definen su función principal de envío y recepción de correos de forma eficiente.

El principal desafío para postscreen es tomar la decisión de si una conexión entrante es con un “zombi” o no. La toma de esta decisión resulta necesaria debido a que muchos zombis evitan el envío de spam al mismo sitio repetidamente. Una vez que decide que un cliente no es un zombi, lo coloca en la lista blanca temporalmente para evitar más retrasos en el correo legítimo.

Postscreen usa una variedad de medidas para reconocer zombis:

a) Postscreen determina si la dirección IP del cliente SMTP remoto está en la lista negra.

b) En segundo lugar, postscreen busca compromisos de protocolo que se realizan para acelerar la entrega. Estos son indicadores adecuados para que el proceso sea capaz de tomar la decisión de si es o no un zombi basándose en mediciones individuales.

Postscreen no inspecciona el contenido del mensaje. El contenido del mensaje puede variar de una entrega a otra, especialmente con los clientes que (también) envían correos electrónicos legítimos. El contenido no es un buen indicador para tomar en cuenta de cara a discernir si el remitente es un -zombi, y ese es el problema en el que se centra postscreen.

6.5.8 SPF EN POSTFIX

SPF (Convenio de Remitentes, del inglés Sender Policy Framework) es una protección contra la falsificación de direcciones en el envío de correo electrónico, autenticando a los servidores de correo electrónico que están autorizados para el envío de mensajes de una organización, evitando así usos de phishing o de correo fraudulento, identifica los servidores de correo SMTP autorizados al envío electrónico a través de los registros de nombres de dominio (DNS).

SPF utiliza el protocolo de comunicación SMTP para la comprobación de los servidores de correo autorizados de una organización al envío de los mensajes electrónicos a un dominio.

SPF hace un registro de nombres de servidores y/o de sus direcciones IP al DNS de un dominio, autorizando a estos servidores de correo al envío de mensajes electrónicos desde su dominio especificado. El receptor del correo electrónico usará la dirección del correo (alojada, en el encabezado de return-path del mensaje), para confirmar que el remitente está autorizado al envío del mensaje.

Cuando un servidor de correo electrónico no se encuentra en un registro SPF, el correo originado por dicho servidor es marcado como "sospechoso", pudiendo ser rechazado o marcado como spam por el receptor del mensaje.

El registro de SPF se aloja en un formato txt en el servidor DNS, este registro es el que tiene la información necesaria para designar el Sender Policy Framework.

Una configuración de registro de SPF se rige por una serie de mecanismos, los cuales son los utilizados para describir el comportamiento que deben de tener los servidores de correo registrados para el dominio de la organización. Además, se utilizan una serie de prefijos que completan las funcionalidades de los mecanismos. A continuación, se describen los mecanismos:

Mecanismo	Nombre
all	Este mecanismo suele ir precedido por los sufijos - y ~, y se suele colocar al final. Su uso, con estas características, es de aprobar o desautorizar los mecanismos anteriores.
a	Capacita a los servidores de correo de nuestro dominio a mandar mensajes de correo electrónico, los equipos que tengan una dirección IP de tipo A registrada en el DNS del dominio. Si no se indicase el dominio, el mecanismo asume que tal dominio es el asociado a la dirección de cuenta de correo electrónico registrado A.
mx	Autoriza al envío de correos electrónicos a los servidores del dominio con una dirección IP inscrita a los registros mx. De no especificar el nombre de dominio, se asocia al dominio del correo electrónico de salida.
ptr	Con este mecanismo, se autoriza el envío de correos electrónicos a los servidores, los cuales tengan una dirección IP cuya resolución inversa pertenezca al dominio. Si no se especifica el dominio, se toma como dominio el propio del correo a enviar.
ip4	Capacita al envido de correos electrónicos a los servidores cuyas direcciones IP sean especificadas o de un rango de IP´s indicados.
ip6	Realiza la misma función descrita anteriormente en el mecanismo de ip4, pero con la salvedad del uso del protocolo ipv6, en vez de ipv4.
include	Es un mecanismo que indica que se realice una búsqueda en otro dominio de algún mecanismo que garantice que el correo electrónico es correcto y debe ser aceptado, estas circunstancias se dan como válidas si el servidor DNS donde se realiza la consulta devuelve un valor de "permitido". Si en el proceso de búsqueda, este dominio no devolviese un valor de "permitido", el proceso prosigue a la siguiente directiva del registro SPF.

Los prefijos de los mecanismos descritos anteriormente son:

Prefijo	Nombre	Descripción
~	Virgulilla o softfail	El mensaje procedente de la dirección IP indicada, no es rechazado, pero si marcado en su cabecera para tener en tratamiento posterior a definir.
–	Guion medio o fail	Rechaza los mensajes electrónicos de un origen dado por una dirección IP.
+	Mas o Pass	Autoriza la dirección IP proporcionada en el archivo de registro.
?	Interrogación o Neutral	Este prefijo se suele utilizar en periodos de prueba. Añade en su cabecera la instrucción “Received-SPF: neutral”.



6.5.9 DKIM EN POSTFIX

Con el fin de reducir la falsificación de correo electrónico y proporcionar más seguridad para una organización, Postfix pude implementar la validación entrante del correo identificado Domain Keys (DKIM) sobre IPv4. Esta tecnología, es un protocolo de autentificación de correo electrónico que actúa comprobando los remitentes autenticados de confianza y ayudan a identificar los que no son como tales.

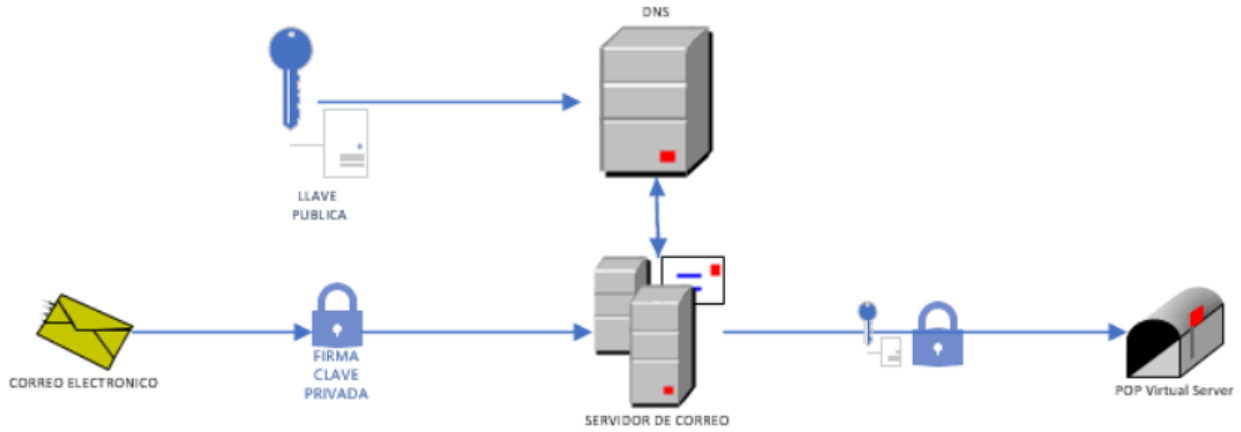
Esta validación de correo electrónico permite a la organización responsabilizarse de la autoría del envió de un correo electrónico por parte de la misma, de manera que el destinatario pueda validar el origen del correo electrónico y así poder evitar la suplantación de la identidad de la organización.

Este mecanismo de autentificación viene por la posibilidad de poder cambiar la cabecera de un mensaje “from”, utilizado para la identificación de un dominio, evitando así el uso fraudulento e indebido de mensajes de una organización y depurando responsabilidades si fuera necesario.

DKIM utiliza mecanismos criptográficos de clave pública para poder permitir el uso de firma electrónica por parte de la organización en los correos electrónicos originados, pudiendo ser legitimado el mensaje electrónico por el receptor del mismo.

Para evitar la manipulación del correo electrónico, DKIM, protege la integridad del mismo de extremo a extremo, insertando un módulo firmante en la cabecera del mensaje sobre el nombre de la organización. A la recepción del mensaje, existe un módulo de comprobación en la firma de DKIM por parte del receptor, que actúa sobre el nombre de la organización, validando la firma obtenida por la clave pública de la organización emisora del correo electrónico, a través de un servidor DNS.

DKIM es independiente del protocolo SMTP, interviniendo sobre las cabeceras y el cuerpo del mensaje.



PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL