Capítulo 8
Configuración de los componentes de transporte

1. Presentación de los servicios de transporte

1.1 Principio de funcionamiento de los servicios de transporte Exchange

Como se ha indicado en los capítulos anteriores, Exchange Server 2013 rompe con las arquitecturas de las versiones anteriores del producto. La integración de las funcionalidades de transporte se beneficia de las mismas ventajas que para los roles **Acces clients (CAS)** y **Buzones (MBX)** e, incluso si el rol **Hub-transport** no se menciona directamente, lo cierto es que la configuración y el funcionamiento interno siguen siendo muy parecidos al de las versiones anteriores.

De esta manera, los componentes de transporte tienen como objetivo el enrutamiento de los mensajes, tanto en el interior como en el exterior de la organización Exchange, gracias a los diferentes mecanismos de enrutamiento.

El servicio frontal de transporte alojado por los servidores de acceso de cliente (CAS), actúa como un proxy SMTP en el tráfico entrante y saliente de la organización Exchange 2013. Este no realiza ningún análisis del contenido y transmite directamente los mensajes al servicio de transporte de un servidor de buzones de mensajes (MBX) 'saludable'.

La selección del servidor de buzones de mensajes se hace sin tener en cuenta ni el nombre, tipo o ubicación de los destinatarios del o de los mensajes.

El enrutamiento de los mensajes se puede hacer entre los diferentes servicios de transporte alojados en los servidores de buzón de mensajes de la organización.

La segmentación de las zonas que permiten el enrutamiento de los mensajes se hace por los grupos de entrega que permiten facilitar el enrutamiento de los mensajes, con el objetivo de mejorar la eficiencia de los intercambios en la infraestructura. Un grupo de entrega puede ser: un grupo de disponibilidad de base de datos, un grupo de entrega de buzones de mensajes, un conector de servidor origen, un servidor de expansión de grupo de distribución…

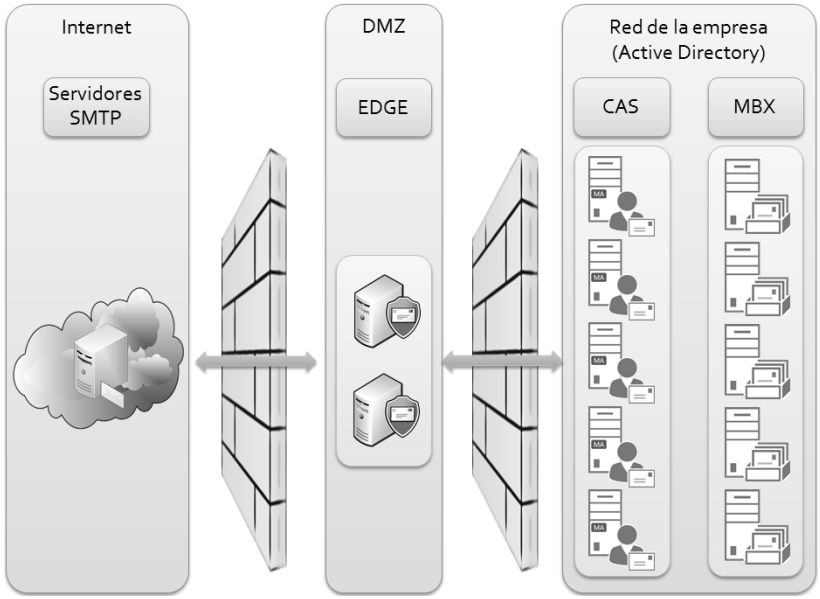
Después del análisis del mensaje, cuando los servidores de buzones de mensajes se deben intercambiar el mensaje que se encuentra en grupos de entrega diferentes, se enruta de nuevo por un intercambio entre los servicios de transporte de diferentes servidores de buzones de mensajes.

Se configura un conector de envío en el servidor de buzones de mensajes, para la entrega del correo al exterior de la organización Exchange, a través del servidor que tiene el rol de acceso de cliente.

Incluso si todavía no está disponible en su versión 2013, el rol **Edge** de las versiones anteriores de Exchange, se puede utilizar para permitir un análisis del flujo de mensajes en **DMZ** (zona despejada).

Observación

La implementación del servidor Edge se tratará en el capítulo Implementación del rol de Transporte Edge de este libro.



La mayor parte de los mecanismos de intercambio en la infraestructura Exchange, se basan en el protocolo **SMTP** (*Simple Mail Transfer Protocol*) como protocolo de transporte, durante las comunicaciones con los dominios de mensajería electrónica en Internet.

1.2 El protocolo SMTP (Simple Mail Transfer Protocol)

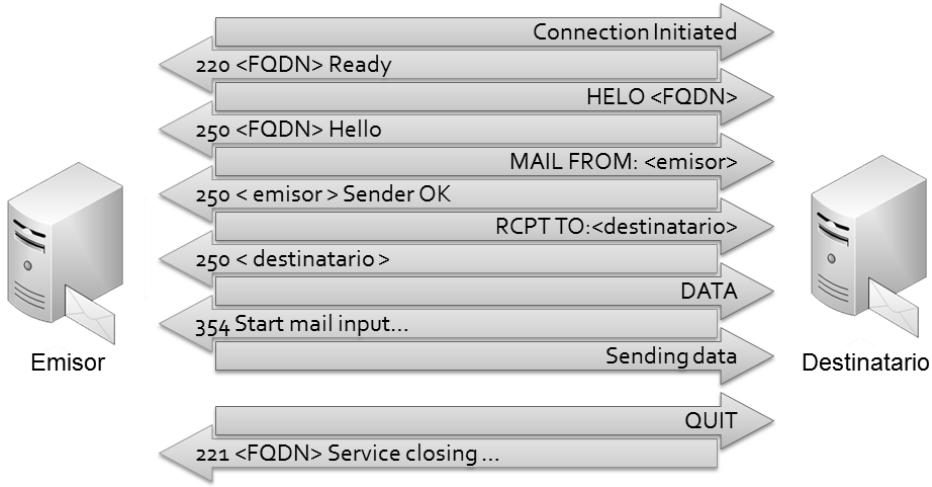
El protocolo **SMTP** asegura las funciones de enrutamiento de los mensajes electrónicos, se encarga de la entrega de los mensajes que le son confiados hasta su destinatario, pero también puede actuar como repetidor si se configura correctamente.

Normalmente asociamos al protocolo SMTP un sistema de cola. En realidad, es una de las grandes ventajas del protocolo y es fundamentalmente asíncrono. Si se envía un e-mail al servidor SMTP y este no puede recuperarlo inmediatamente ya que el servidor SMTP de destino está en mantenimiento durante varias horas, el mensaje se va a almacenar en una cola y el servidor intentará regularmente recuperar el mensaje.

El protocolo SMTP utiliza el puerto TCP 25 por defecto y se ha convertido en el protocolo estándar de transferencia de mensajes electrónicos entre los servidores y los clientes.

Como su nombre indica (*Simple Mail Transfer Protocol*), el protocolo es muy básico. No tenía por objetivo durante su diseño convertirse en la norma de transferencia de mensajes electrónicos a nivel mundial. Tiene varios problemas de diseño importantes, particularmente a nivel de seguridad y de escalabilidad. La implementación de un servidor SMTP hace obligatorio prestar una atención particular para evitar que su servidor se convierta en el Gateway preferido de los spammers.

A continuación se muestra un ejemplo de intercambio clásico entre dos servidores de mensajería electrónica que usan el protocolo SMTP.



A continuación se muestra una lista de los comandos SMTP más habituales:

– **HELO <fqdn>**: identifica al servidor emisor.
– **MAIL FROM: <emisor>**: identifica al emisor del mensaje.
– **RCPT TO: <destinatario>**: identifica al destinatario del mensaje.
– **DATA**: envía el mensaje al servidor de destino.
– **RSET**: abandona el envío del mensaje actual.

– **VRFY <cadena >**: comprueba que el destinatario es válido en el servidor de destino (este comando normalmente está bloqueado para evitar la constitución de una lista de spam).
– **HELP**: muestra la lista de los comandos SMTP soportados.
– **QUIT**: desconecta la sesión.
– **TURN**: envía los mensajes en lista de espera.

1.3 El protocolo ESMTP (Extended Simple Mail Transfer Protocol)

Para contrarrestar las lagunas del SMTP, el protocolo **ESMTP** permite extender los comandos SMTP, integrando fundamentalmente la autentificación de hosts y el cifrado. La distinción se hace durante la conexión que utiliza la cadena de caracteres HELO para el SMTP y EHLO para el ESMTP.

El protocolo ESMTP permite al servidor de destino ofrecer al servidor emisor la lista de comandos con los que es compatible. En caso de que el servidor de destino no sea compatible con el protocolo ESMTP, la conexión se restablece con ayuda del protocolo SMTP.

A continuación se muestra una lista de los comandos ESMTP más habituales:

- **EHLO <fqdn>**: identifica al emisor y el protocolo ESMTP.
- **ATRN**: se ejecuta si la sesión se autentifica.
- **ETRN**: idéntica a TURN pero específica al host remoto al que será remitido el mensaje.
- **PIPELINING**: envía por lotes los comandos SMTP, sin esperar la respuesta del destinatario.
- **CHUNKING**: envía los mensajes MIME de tamaños grandes.
- **STARTTLS**: establece una conexión SSL entre el cliente y el servidor.
- **AUTH**: proporciona una forma de autentificación SASL para autentificarse con ayuda de Kerberos y NTLM.

1.4 Mecanismo de envío de un e-mail

Para enviar un e-mail, es necesario que el servidor de mensajería electrónica conozca la dirección IP del servidor SMTP de destino. Para esto puede elegir entre delegar la entrega a un smart-host o entregar el mensaje él mismo.

En caso de delegación de entrega, el conjunto de mensajes electrónicos que se debe enviar, se va a transferir a otro servidor SMTP que será el encargado de la entrega final al servidor de destino. Este rol se puede asimilar al rol Edge en la infraestructura Exchange 2013.

En caso de la entrega directa, el servidor SMTP va a preguntar al espacio de nombres DNS del dominio de destino. Si se envía un e-mail a angelms@ediciones-eni.com, el servidor va a preguntar al espacio de nombre ediciones-eni.com. En el espacio de nombres DNS, el servidor SMTP emisor va a buscar una entrada de tipo MX que representa un servidor de mensajería electrónica del dominio remoto. El servidor DNS va a reenviar la dirección IP del servidor de mensajería electrónica de destino y envía el e-mail.

Cuando se ha enviado el e-mail, aparece el problema de la confianza establecida por el servidor de destino a nuestro e-mail. Esta confianza depende del contenido del e-mail y de la confianza asignada al servidor emisor. Si esta confianza no es elevada, el mensaje corre el riesgo de ser catalogado como spam.