



Soluciones Appliance

SERVIDOR MTA ULTRA SEGURO

CIFRADO TLS-SSL

SALS-CHROOT-MYSQL

EN ALTA DISPONIBILIDAD Y ESCALABLE

ÍNDICE DE CONTENIDO

| | |
|-----------------------------------|----------|
| 1 Seguridad..... | 1 |
| 1.1 Cifrado de claves..... | 2 |
| 1.2 TLS y SSL..... | 2 |
| 2 Alta disponibilidad..... | 3 |
| 2.1 Heartbeat..... | 3 |
| 2.2 DRBD..... | 4 |
| 3 escalabilidad..... | 5 |

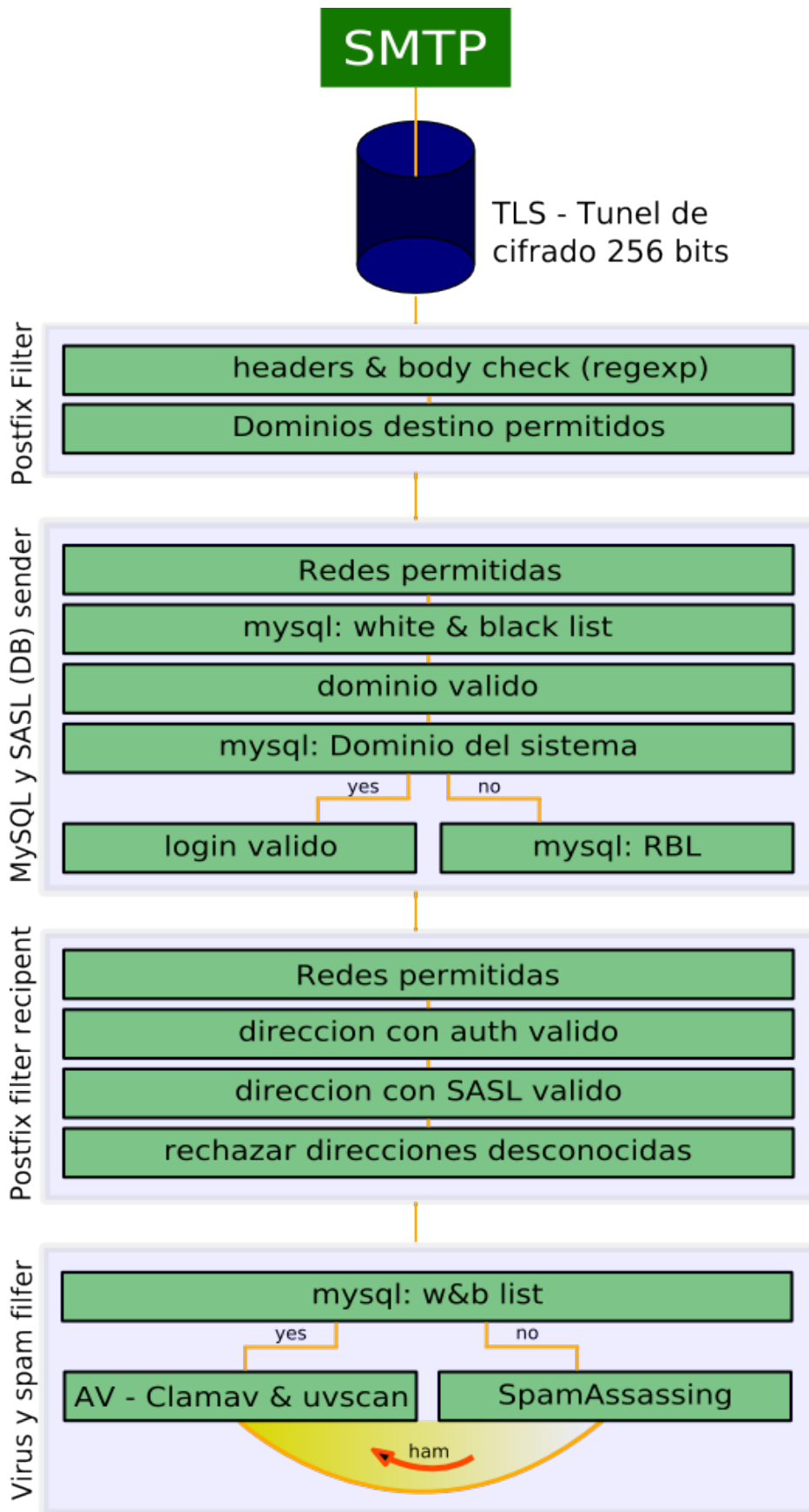
1 SEGURIDAD

La seguridad es el principal aspecto a tomar en cuenta en esta instalación. Si bien la arquitectura del servidor ya permite una seguridad aceptable a nivel de redes se tiene que tomar en cuenta la seguridad en la aplicación y validación de usuarios.

Muchos servidores de correo comúnmente instalados tienen fallos en su configuración por lo que permite utilizarlos como relay o falsificar la identidad de otros usuarios del propio dominio, sin encriptación en la autenticación y en el envío .

Con esta configuración se pretende controlar muy eficazmente que todos los correos que lleguen o se envíen por el servidor bajo un dominio o multidominio sea autenticado fielmente y certifiquen el remitente y el receptor de los correos.

En la siguiente gráfica podemos apreciar los controles de seguridad y filtros al que expuesto un correo recibido.



1.1 CIFRADO DE CLAVES

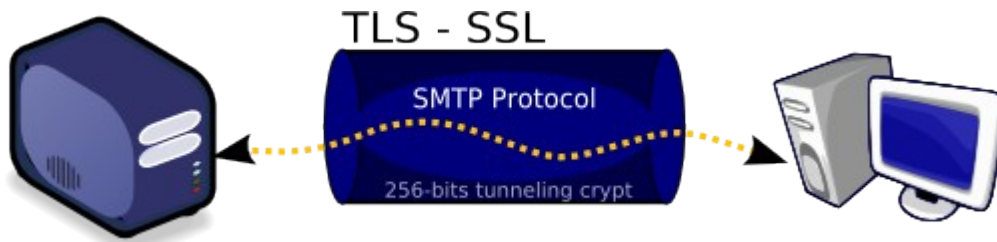
La configuración de postfix contra SASL y MySQL no permite mantener las claves cifradas en el servidor por lo que no cumpliría con la ley de protección de datos. Para solucionar este problema utilizamos las propias funciones de MySQL para cifrar y descifrar.

Encryption Functions - <http://dev.mysql.com/doc/refman/4.1/en/encryption-functions.html>

The functions in this section encrypt and decrypt data values. If you want to store results from an encryption function that might contain arbitrary byte values, use a `BLOB` column rather than a `CHAR` or `VARCHAR` column to avoid potential problems with trailing space removal that would change data values.

1.2 TLS Y SSL

Cuando se realiza una conexión para autenticación de usuario (de otro modo no puede enviar un correo bajo el dominio) se inicia una conexión TLS que supone un túnel de cifrado de 256 bits.

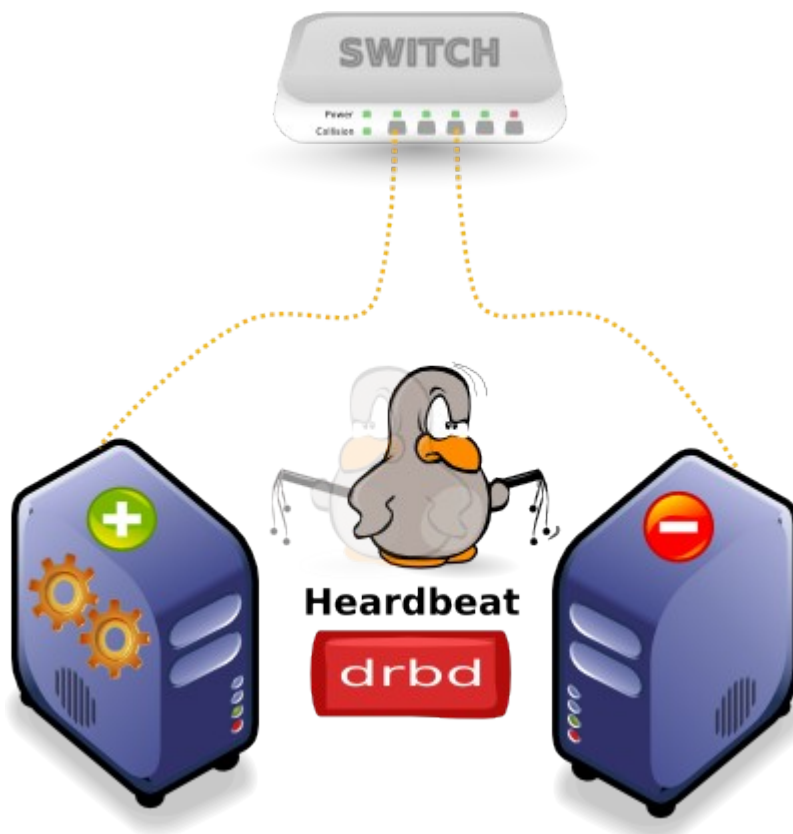


Todo el protocolo de SMTP pasa a través de este túnel impidiendo cualquier técnica de sniffing ya que el cifrado inicia y termina en el servidor y la maquina cliente directamente sin que ningún dispositivo que se encuentre entre los mismos pueda leer el dicho protocolo.

2 ALTA DISPONIBILIDAD

2.1 HEARDBEAT

Configurado exclusivamente para este tipo de servidor optimizamos de la mejor forma posible los recursos de la red y de hardware. Esta parte del producto tiene como objetivo analizar el estado de los servidores en todo momento y responder en cada cambio de estado.



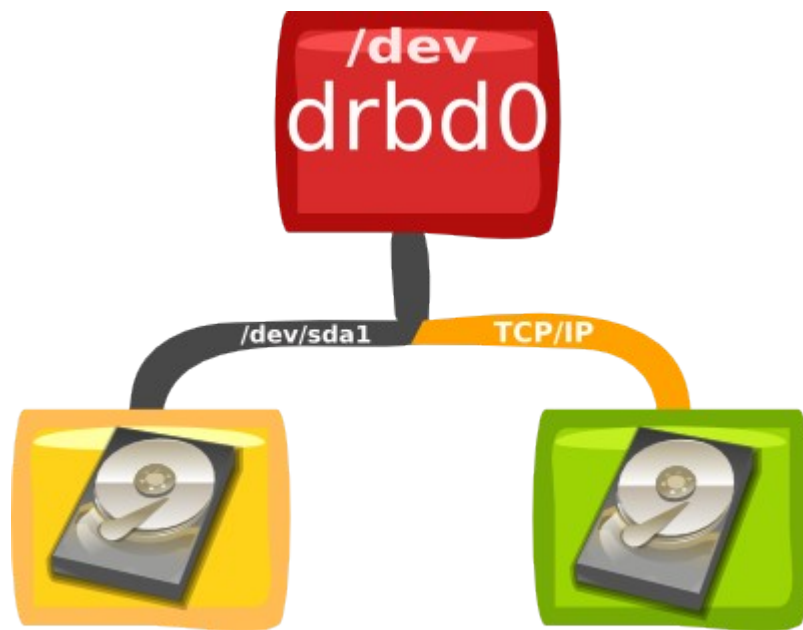
Un de los servidores esta en activo y el otro en pasivo. Heartbeat, instalado y configurado en ambos equipos, se encarga de mantener la relación de activo-pasivo evitando que los dos entren en estado activo o pasivo al mismo tiempo. Esta configuración de verificación de estado es personalizada según el entorno donde estén instalados los servidores (LAN, MAN, WAN, Internet ...)

2.2 DRBD

DRDB es una tecnología avanzada que permite un nivel de redundancia de datos en tiempo real, algo que era muy difícil de conseguir con otros sistemas como rsync ya que este no puede estar trabajando en tiempo real el 100% del tiempo por que su consumo de memoria y CPU sería demasiado costoso.

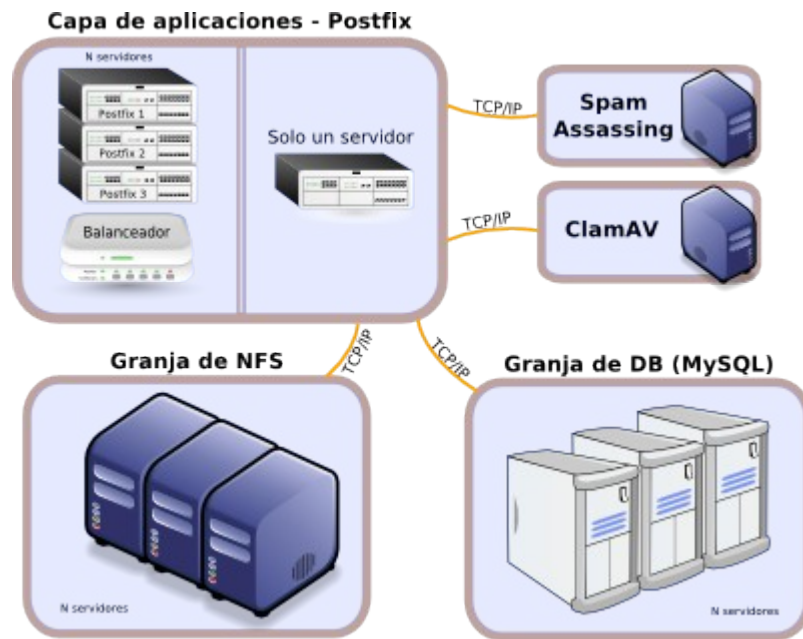
DRDB nos permite mantener los mismos ficheros inalterables es como si se tratara de un RAID-1 virtual por RED. Con unos módulos compilados para el kernel se crea dispositivos llamados drbd0/15 que se convierten en unidades de bloques como cualquier otro dispositivo de almacenamiento.

Una vez cargados y configurados se conecta ambos servidores, uno en activo y otro en pasivo, se sincronizan (al igual que un RAID) y empiezan a trabajar. El primero cada vez que escribe algo en su partición drbd la misma escritura se realiza en la partición física que tiene en sus discos duros y esa misma escritura las envía por TCP/IP al otro servidor que al llegar se escribe en su disco duro.



3 ESCALABILIDAD

Al ser un sistema completamente modular podemos escalarlo sin limite con distintas técnicas de escalabilidad. Se puede utilizar varios servidores con las mismas características, servidores poco potentes, que reducen mucho los costes y reparte la carga en cada uno de estos equipos.



Si bien cada proceso se diferencia por su forma de consumir recursos (CPU, memoria, HD, DB) Diseñamos zonas según la forma de consumo, aplicando el diseño de este gráfico podríamos soportar miles de usuarios y de una manea mas eficiente que si colocamos dos o tres servidores con la misma configuración y con un balanceador delante, podemos aumentar el numero de nodos según el proceso que mas consuma o realmente requiera mas capacidad (como puede ser el anti-virus en una ola de virus como *blaster*)