**Instalación de un servidor de correo seguro**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

[**1. Índice:**](#_lmwzrhyaxgtw) **2**

[**2. Preparación del entorno**](#_g59i8ewd3ed3) **3**

[**2.1 Configurar los registros DNS para el servidor de correo**](#_gq6dpe40wu9t) **3**

[**2.2 Instalación de Postfix**](#_gckqfh7dpag7) **5**

[**2.3 Instalación de Dovecot**](#_bkl7lgnxpt0s) **7**

[**2.4 Instalación de roundcube**](#_rtbv0nla4cr9) **10**

[**3. Protocolos de suplantación de identidad en correos electrónicos**](#_1t8pfbxa8p5t) **12**

[**3.1 Configuración de Sender Policy Framework SPF para correo enviado**](#_zhw382swz5dv) **12**

[**3.1 Configuración de Sender Policy Framework SPF para correo recibido**](#_nmrkt4kpnd95) **12**

[**4. Configuración de DomainKeys Identified Mail DKIM**](#_cw4npiujwkm) **13**

[**5. Configuración de Domain-based Message Authentication, Reporting & Conformance DMARC**](#_6a0ki6wef0zu) **15**

[**6. Instalación de un sistema antispam externo**](#_mwjesy7e8lsf) **19**

# **2. Preparación del entorno**

Antes de instalar Postfix vamos a realizar una serie de modificaciones en el sistema para que esté todo correcto

Si nuestro servidor no tiene un nombre FQDN, podemos utilizar el comando hostnamectl para asignarle uno.

sudo hostnamectl set-hostname mail.cursobastionado.com

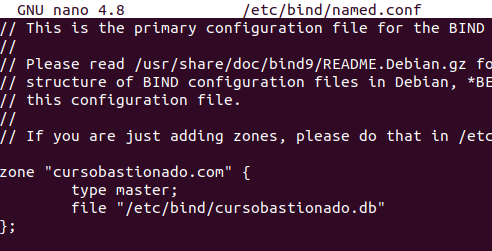


## **2.1 Configurar los registros DNS para el servidor de correo**

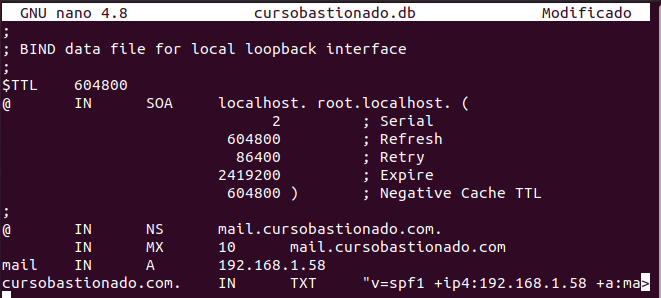
Necesitamos configurar los registros DNS de la red e incluir entradas del tipo MX para especificar los servidores de correo.

Localizaremos y editaremos el archivo /etc/bind/named.conf.local para indicarle como se llama nuestra “zona” y configurarla. Aquí estableceremos cual va a ser nuestro dominio. En nuestro caso hemos elegido el dominio “cursobastionado.com”.

Introduciremos el siguiente código en el archivo named.conf.local



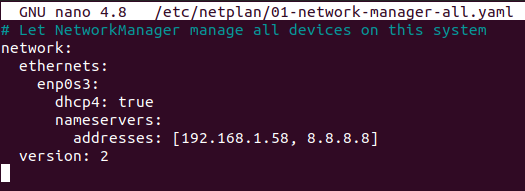
Creamos el fichero cursobastionado.db y añadimos lo siguiente

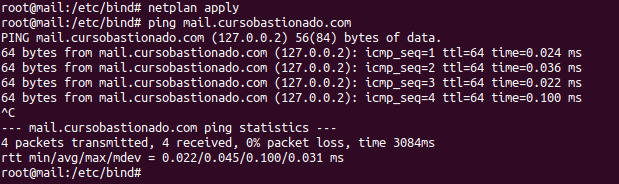


Para poder trabajar con el servidor de correo en Ubuntu de forma local, cambiaremos las DNS de nuestra máquina y le introduciremos como DNS la IP de la propia máquina.

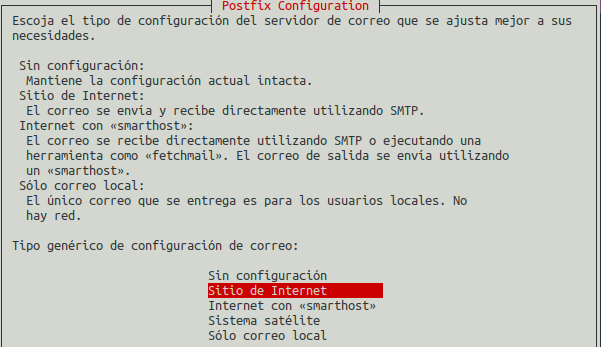
Editamos el fichero .yaml y añadimos la sección nameservers con la dirección ip de nuestra máquina virtual Ubuntu. Recordar que no se puede utilizar el tabulador para crear los espacios.

Quedaria algo asi

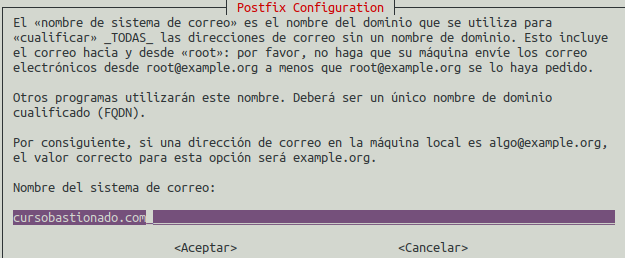




## **2.2 Instalación de Postfix**



Pondremos el nombre del dominio que hemos elegido:

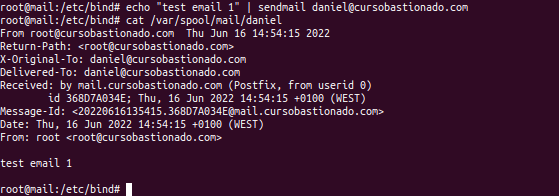


Y comprobamos la versión a la vez que observamos el puerto de escucha abierto





Cuando instalamos Postfix, el binario de sendmail se encuentra en /usr/sbin/sendmail. Podemos utilizar este binario para probar el envío de correo a una cuenta de esta forma:



Para agilizar la configuración y evitar fallos durante la modificación de postfix, vamos a descargarnos el fichero main.cf del siguiente enlace y lo cambiaremos por el que tenemos por defecto en nuestra máquina Ubuntu.

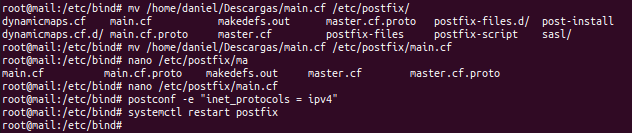
<https://owncloud.areaproject.com/index.php/s/4Zo4dcv3026HQBK>

El fichero viene configurado para el servidor con nombre mail.cursobastionado.com

Movemos el fichero main.cf original a main.cf\_backup y creamos el nuevo fichero con el contenido del que hemos descargado.

Ahora si quisiéramos que nuestro servidor solamente actuara en ipv4 podríamos ejecutar el

siguiente comando:



Si el servidor fuera a contener más de un dominio desde el que se pudiera enviar correo tendríamos que configurar los virtual\_mailbox.

Vamos a dejarlo listo para un futuro y configuraremos solamente nuestro dominio.

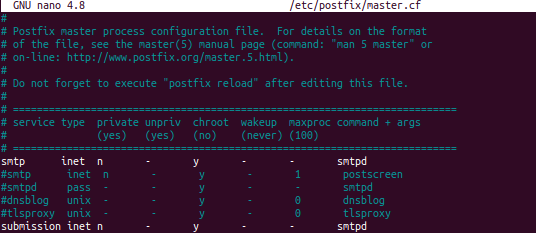
Editaremos el fichero necesario. Este fichero se llama /etc/postfix/virtual\_mailbox\_domains.

Creamos el fichero y añadimos al cursobastionado.com dentro del fichero.



Ahora vamos a instalar dovecot para permitir que los clientes gestores de correo tipo Outlook o incluso gestores de webmail puedan enviar y recibir correo utilizando nuestro servidor, para ello, primero necesitamos descomentar la línea submission den fichero master.cf

Editamos /etc/postfix/master.cf para activar el servicio SMTP y descomentamos la línea submission

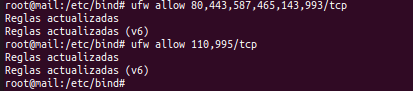


Ubuntu no lleva activado el firewall por defecto. Si lo tenemos activado, necesitamos abrir los puertos siguientes para acceder a webmail, recibir y enviar correo.

Si utilizamos POP3 para gestionar el correo, necesitamos abrir también el puerto 110 y 995.

Si viéramos ahora los puertos en escucha de postfix veríamos el puerto 587 (Submission)

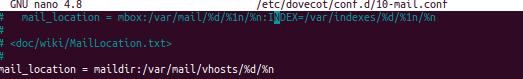
escuchando, el cuál permitiría conexiones mediante encriptación TLS utilizando certificados.



## **2.3 Instalación de Dovecot**

Editamos el fichero /etc/dovecot/conf.d/10-mail.conf para decirle a Dovecot el directorio donde tiene que buscar los correos.

Cambiamos la línea que viene por defecto ya que antes hemos activado los virtual\_mailbox



Ahora debemos de crear el subdirectorio del dominio dentro de /var/mail/vhosts.

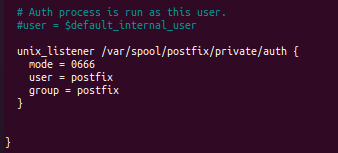
Creamos el usuario y grupo Vmail para el servicio de dovecot.

Asignamos los derechos del directorio al usuario y grupo creado.

Y editamos el fichero de Dovecot 10-master.conf y activamos los servicios imaps, pop3s y lmpt



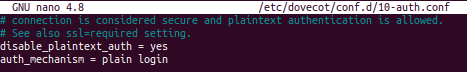


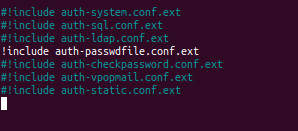


Configuramos Dovecot para usar autenticación segura para ello editamos el fichero 10-auth.conf.

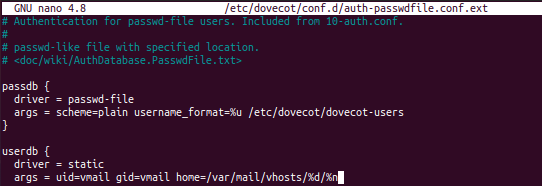
Buscamos la línea # disable\_plaintext\_auth = yes y la descomentamos.

Buscamos la línea auth\_mechanisms = plain y la cambiamos por auth\_mechanisms = plain login

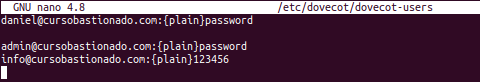




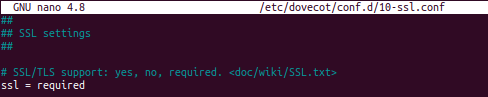
Editamos el fichero de contraseñas de Dovecot, auth-passwdfile.conf.ext sudo nano /etc/dovecot/conf.d/auth-passwdfile.conf.ext Y realizamos estas modificaciones al fichero:



Creamos el fichero de contraseñas /etc/dovecot/dovecot-users. Este fichero es una base de datos en texto sin cifrar.

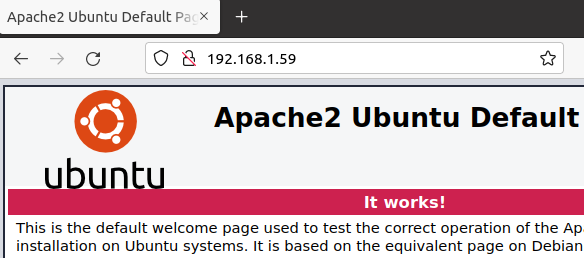


Configuramos Dovecot para usar el certificado SSL. Abrimos el fichero /etc/dovecot/conf.d/10-ssl.conf y cambiamos la línea ssl = yes por ssl = required



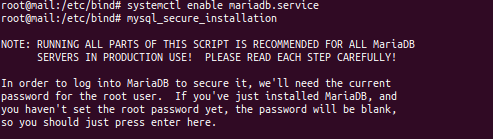
## **2.4 Instalación de roundcube**

Para poder instalar un servidor de correo en Ubuntu que sea accesible vía web es indispensable instalar Apache.

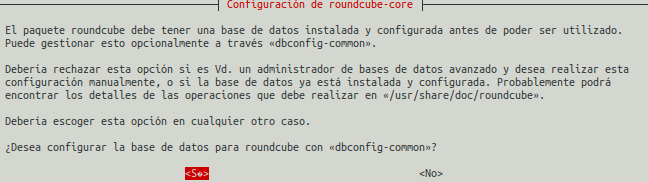


Ahora instalaremos los paquetes necesarios de php para el cliente de correo roundcube y sus dependencias.

Instalaremos el servidor de bases de datos, por ejemplo, maría-db, activamos MariaDB para que se ejecute en el inicio y securizamos la instalación de maría-db

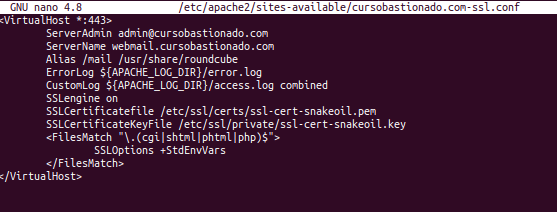


Seguidamente podemos realizar la instalación del cliente dovecot apt install -y roundcube Presionamos ENTER para configurar la base de datos que se utilizará con Roundcube

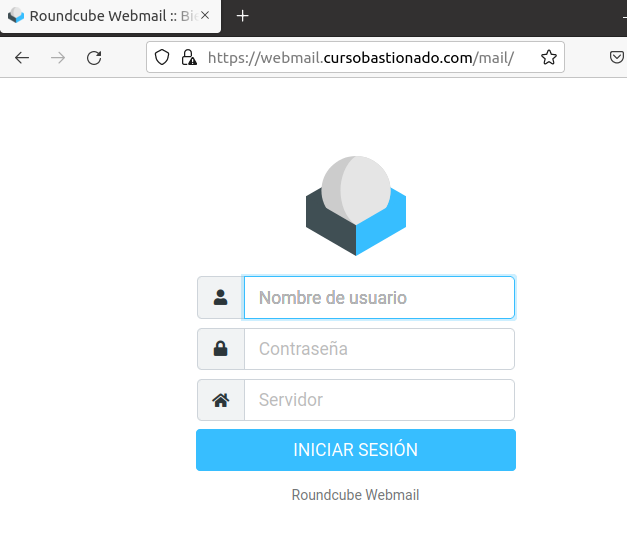


Creamos un fichero de configuración ssl para nuestro dominio en el servidor apache. $ sudo nano /etc/apache2/sites-available/cursobastionado.com-ssl.conf

Y le ponemos el siguiente contenido



Comprobamos



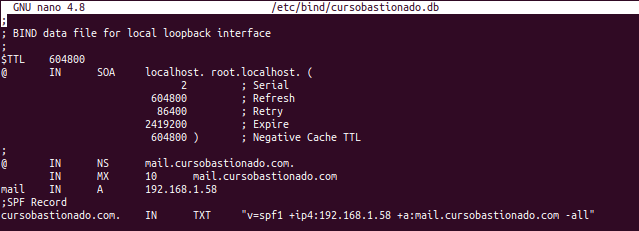
# **3. Protocolos de suplantación de identidad en correos electrónicos**

## **3.1 Configuración de Sender Policy Framework SPF para correo enviado**

La protección SPF se encarga de comprobar los servidores autorizados para enviar correos electrónicos a nombre de un dominio. Para ello, el servidor receptor comprobará en el DNS del dominio la lista de equipos permitidos para dicho fin.

Para que pueda llevarse a cabo la comprobación SPF, se debe registrar en el DNS de tu dominio qué equipos autorizas para que envíen correos electrónicos en tu nombre.

Un ejemplo simple para la configuración SPF en el servidor DNS de cursobastionado.com podría ser el siguiente, donde se indican en los parámetros ip4 los equipos autorizados.



## **3.1 Configuración de Sender Policy Framework SPF para correo recibido**

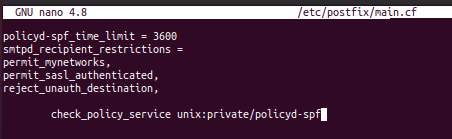
Primero, instalaremos los paquetes requeridos y editaremos el fichero de Postfix

Y añadiremos las siguientes líneas al final del fichero, las cuales le dicen a Postfix que inicie el demonio SPF policy cuando inicie Postfix.



Salvamos y cerramos el fichero. Ahora, editamos el fichero main.cf de Postfix. Añadiremos las siguientes líneas al final del fichero.

La primera línea especifica el timeout, las siguientes líneas imponen una restricción a los mensajes entrantes, rechazando los mensajes no autorizados y chequeando los registros SPF.

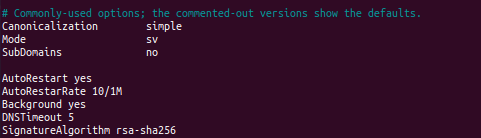


# **4. Configuración de DomainKeys Identified Mail DKIM**

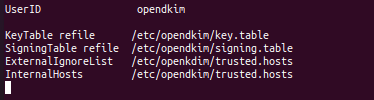
Instalación de opendkim en el servidor, ahora añadimos al usuario postfix al grupo opendkim



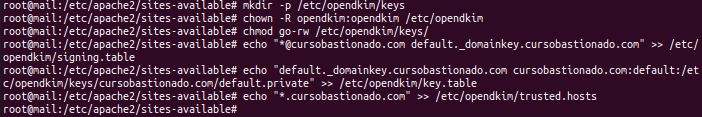
Editamos el archivo /etc/opendkim.conf y descomentamos las siguientes líneas y añadimos las siguientes líneas debajo de Subdomains No



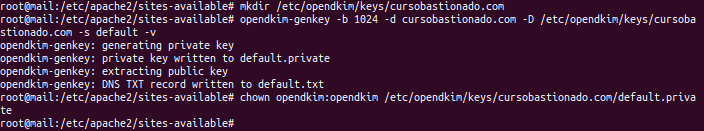
Añadir estas líneas al final del archivo, debajo de UserID opendkim



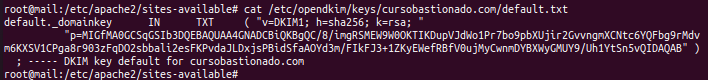
Almacenamos el archivo con esos cambios. Ahora haremos los archivos de configuración, digamos que será para nuestro dominio cursobastionado.com. Primero creamos la estructura de directorios donde se guardarán las claves privadas. También indicamos donde estará la llave privada y lo añadimos a trusted.hosts



Generamos las claves para el dominio cursobastionado.com



Listo, en el archivo default.txt tendremos la llave DKIM



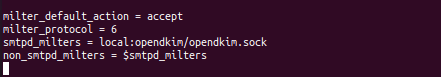
Ahora lo que tenemos que hacer es en nuestro DNS, añadir el registro TXT para el host llamado default.\_domainkey y pegar el contenido que está entre los paréntesis.



Volvemos a editar /etc/opendkim.conf



Ahora editamos /etc/postfix/main.cf y al final de todo añadimos las líneas:

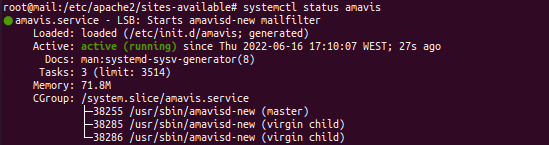


# **5. Configuración de Domain-based Message Authentication, Reporting & Conformance DMARC**

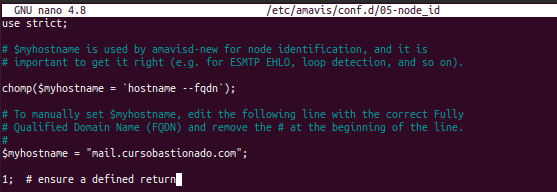
Añadimos nuestro registro DMARC anterior al servidor dns.



Para instalar amavis ejecutaremos el siguiente comando, una vez que se ha instalado, arranca automáticamente



Fijamos la variable $myhostname con el nombre del servidor



Amavis trabaja como un proxy SMTP. Los correos llegan a Amavis a través de smtp, los procesa y los devuelve al MTA mediante otra conexión smtp. Editamos el fichero de configuración de postfix main.cf

Añadimos las siguientes líneas al final del fichero.

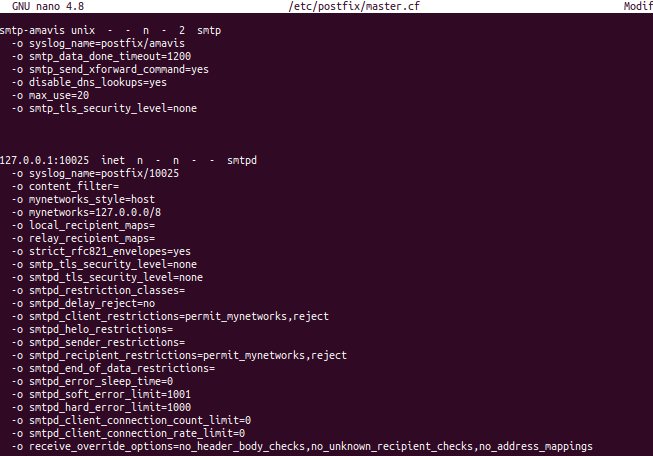


Con la primera línea le decimos a Postfix que mande todo el correo entrante a Amavis que estará escuchando en el puerto 10024.

Con la segunda línea hacemos que Postfix espere a que el mensaje entero haya sido recibido. Esto previenen que clientes con mala conexión tengan problemas de envío.

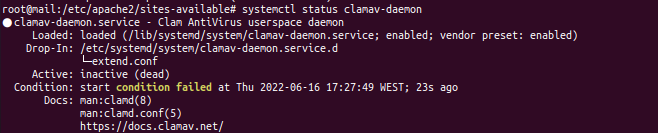
Para finalizar reiniciamos postfix.

Ahora abrimos el fichero master.cf sudo nano /etc/postfix/master.cf Y añadimos el siguiente código al final del fichero

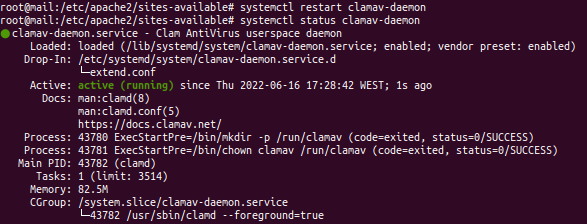


Ahora que Postfix puede pasar los mensajes entrantes a Amavis, necesitamos instalar el antivirus CalmAV e integrarlo con Amavis para que los mensajes entrantes sean escaneados.

Comprobamos el servicio del antivirus

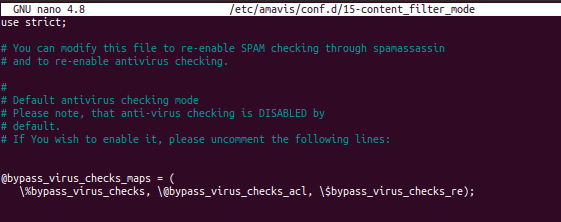


Donde vemos que el servicio ha fallado en el inicio porque ha intentado iniciar antes de descargarse los ficheros con las firmas de los virus, por lo tanto procedemos a activarlo nuevamente



Seguidamente procedemos a activar el chequeo de virus en Amavis.

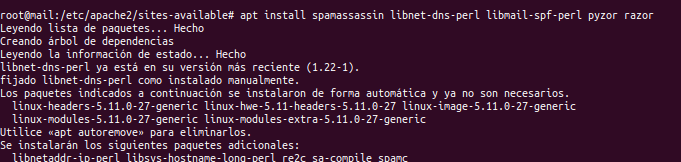
Descomentamos las siguientes líenas para activar el chequeo.



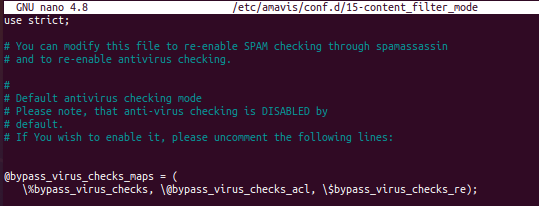
Reiniciamos Amavis y ClamAV para que se apliquen los cambios. Podemos ver que ahora Amavis está usando ClamAV para escanear virus.



Para activar el chequeo de spam en Amavis, instalaremos SpamAssassin con los siguientes paquetes



Editamos el fichero de configuración de Amavis y descomentamos las siguientes líneas para activar el chequeo de spam.



# **6. Instalación de un sistema antispam externo**

En esta práctica vamos a realizar la configuración de un sistema antispam externo al servidor del correo electrónico que hemos configurado anteriormente.

Para este caso vamos a utilizar una distribución específica opensource llamada mailcleaner que descargaremos de la página www.mailcleaner.org

Nos descargaremos directamente la máquina virtual y la importaremos en nuestro entorno de virtualización.

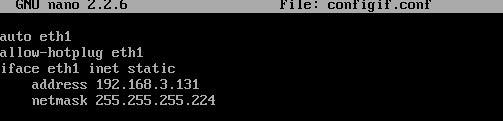
Los datos de la máquina virtual son los siguientes: Account for web interface access: admin Account for shell access: root All passwords: MCPassw0rd

La configuración de la máquina virtual requiere 2 tarjetas de red, una de ellas será la red WAN con acceso a internet y la otra tarjeta será la red LAN desde la que accederemos a su configuración. Para la red WAN he elegido una red Bridge y para la red LAN una red Host-Only.

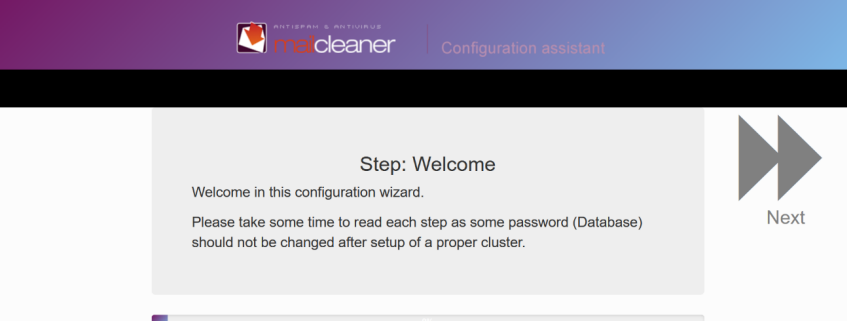
Lo primero que haremos será entrar desde nuestro entorno de virtualización en la máquina virtual y configurar la dirección ip asignada a la tarjeta de red LAN.

En mi caso le pondré la dirección 192.168.3.131/27

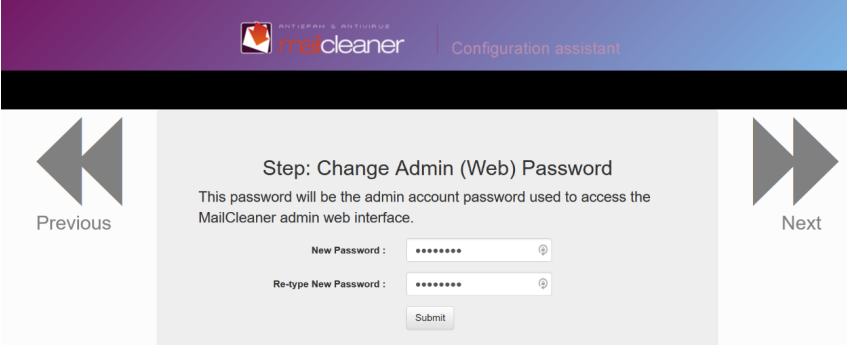
Realizamos una copia de seguridad del archivo /etc/network/interfaces.d/configif.conf y seguidamente lo modificamos poniéndole los siguientes datos.



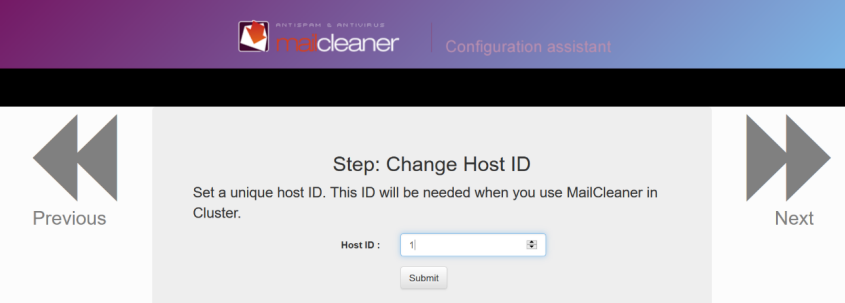
Cuando arrancamos la máquina virtual podemos acceder al configurador vía web



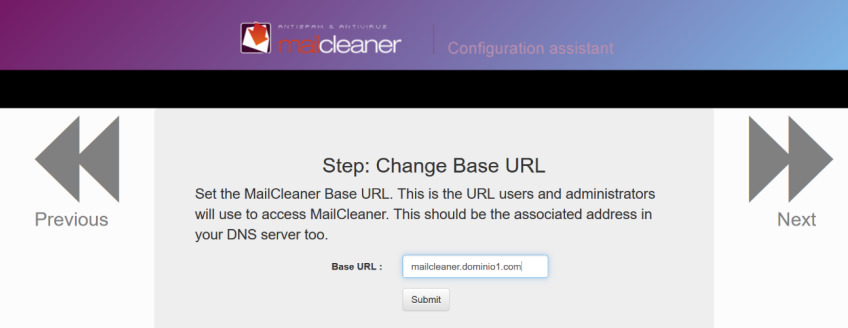
Seguimos el asistente, primero cambiamos la contraseña de administrador y pulsamos sobre el botón “Submit” para aplicar el cambio



Asignaremos un número de Host ID a la instalación

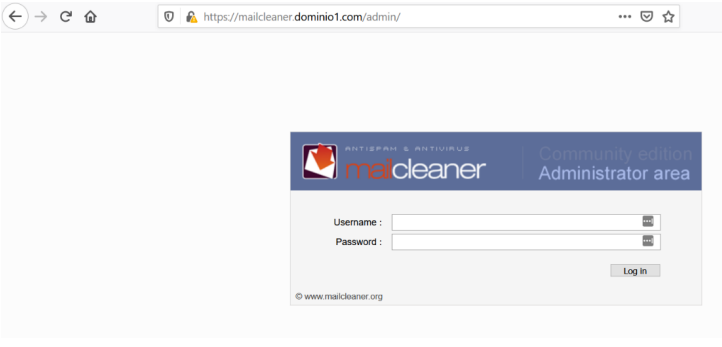


Asignamos un nombre a nuestra nueva máquina. Le he puesto mailcleaner.dominio1.com

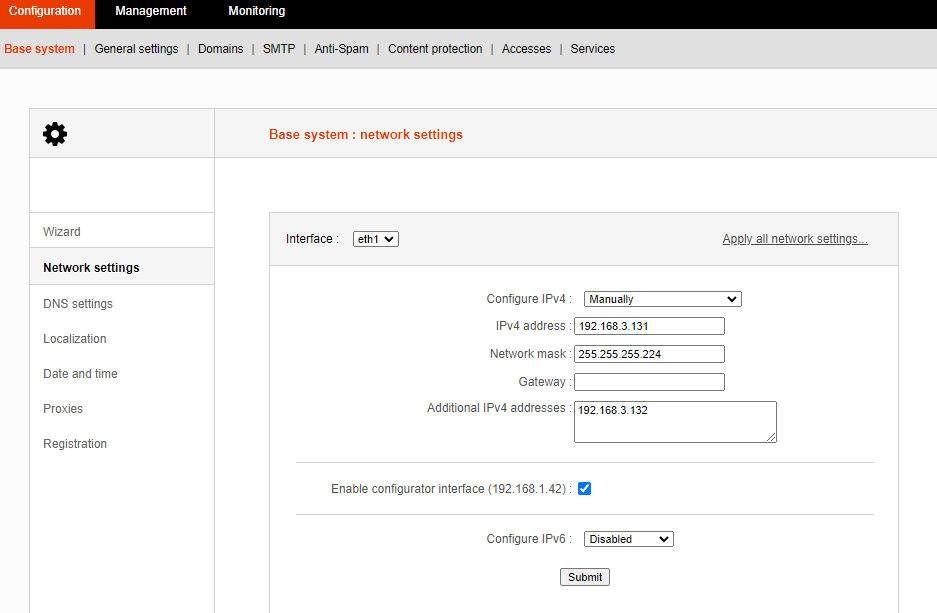


Finalizada la configuración, tendremos que añadir la entrada dns 192.168.3.131 mailcleaner.dominio1.com en nuestro fichero hosts de Windows para que nos resuelva el nombre a la dirección ip.

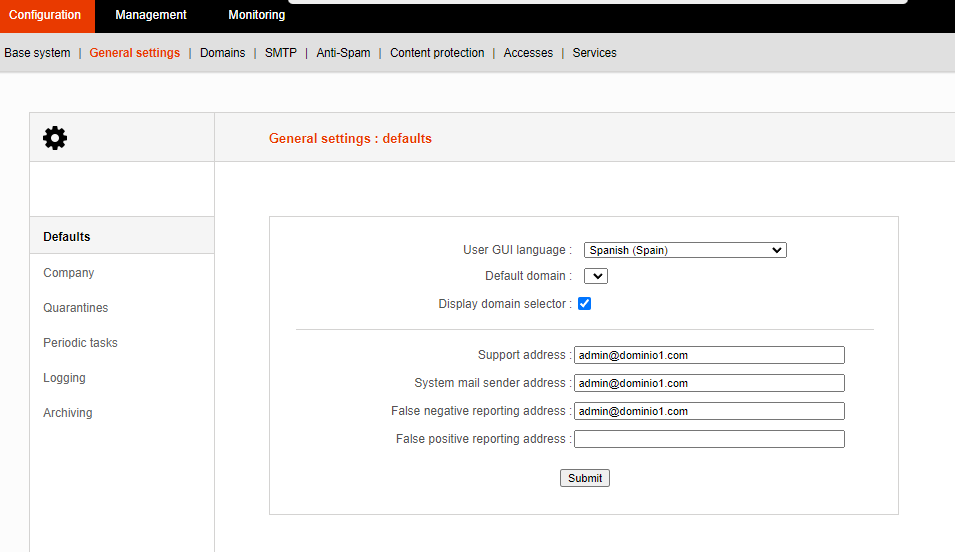
Ahora podremos acceder a su configuración mediante la siguiente URL.



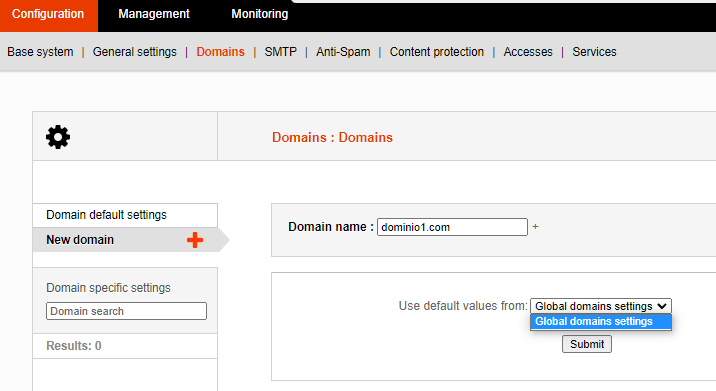
Podremos introducir los datos de la tarjeta de red eth1, seleccionaremos los servidores DNS.

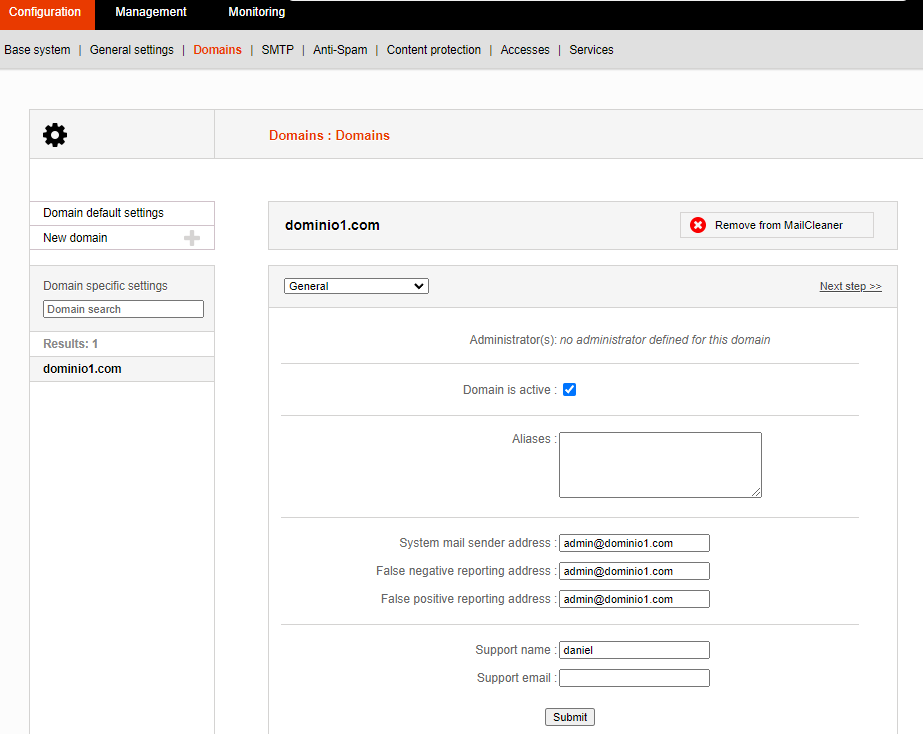


Seguidamente pasamos a “General Settings” y configuramos la dirección de email donde vamos a recibir la información de reportes del sistema, etc

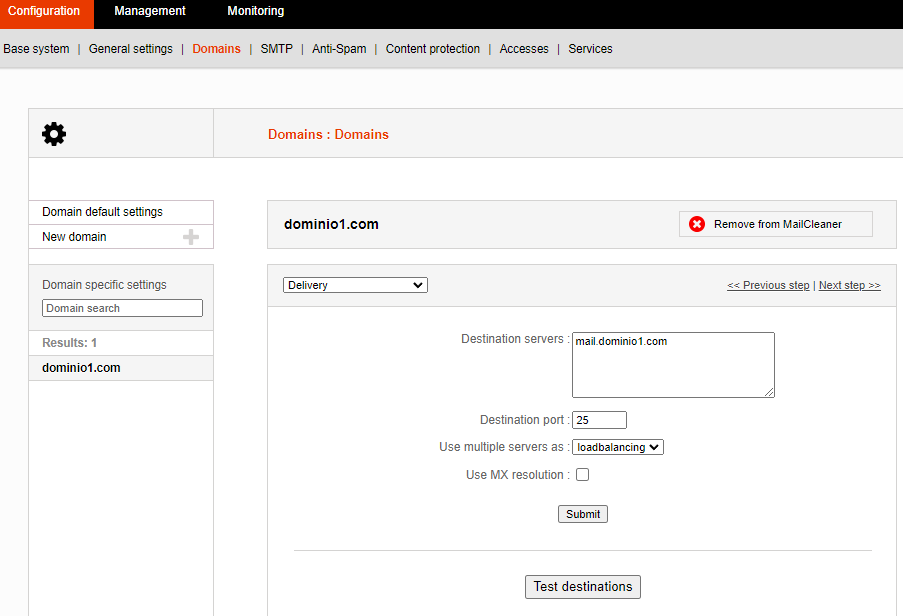


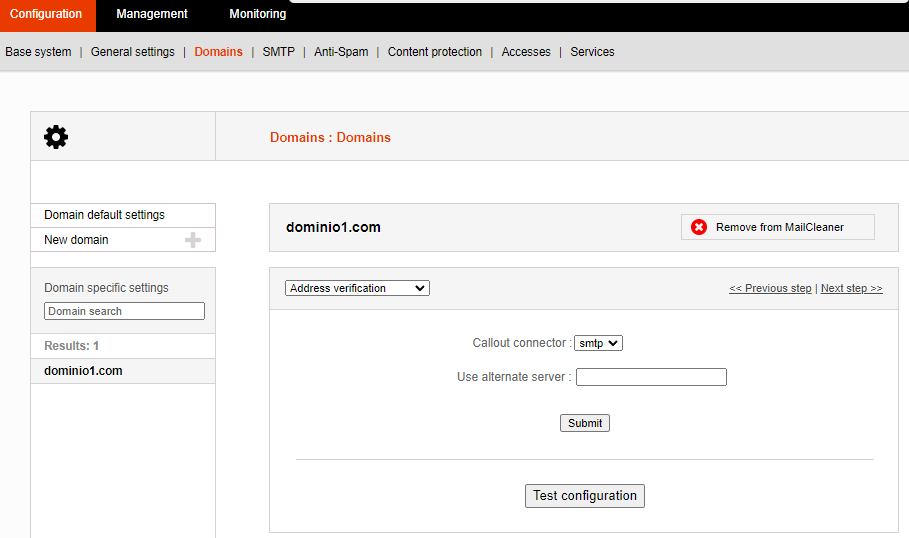
Pasamos a la parte más importante de configuración. Ahora daremos de alta en el sistema a nuestro dominio “dominio1.com”.



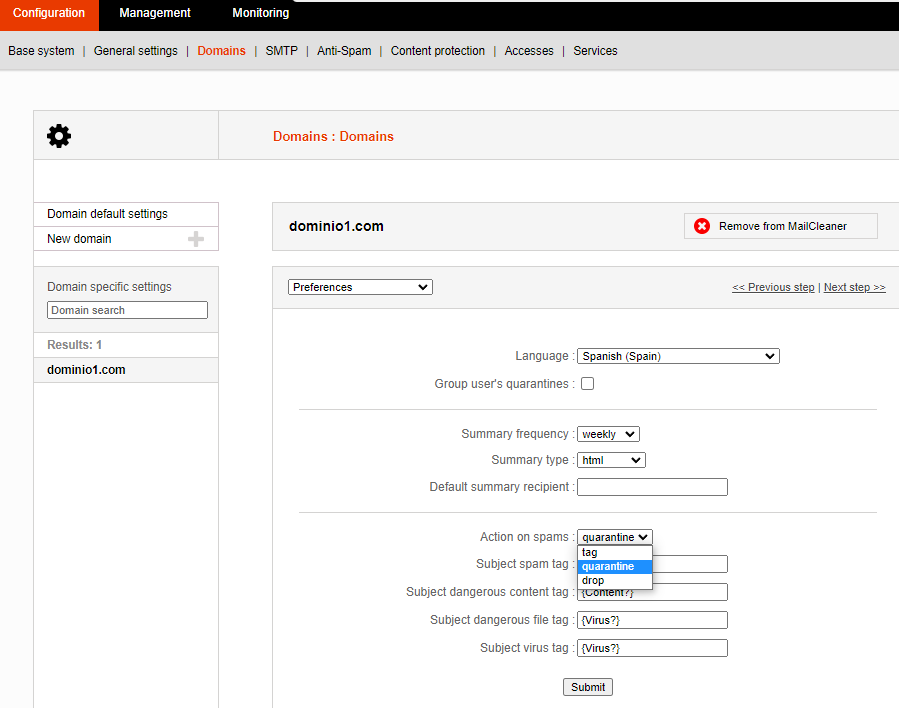


En la siguiente sección de configuración debemos de especificar el servidor de correo al que mailcleaner enviará los correos del dominio dominio1.com después de que los haya comprobado.

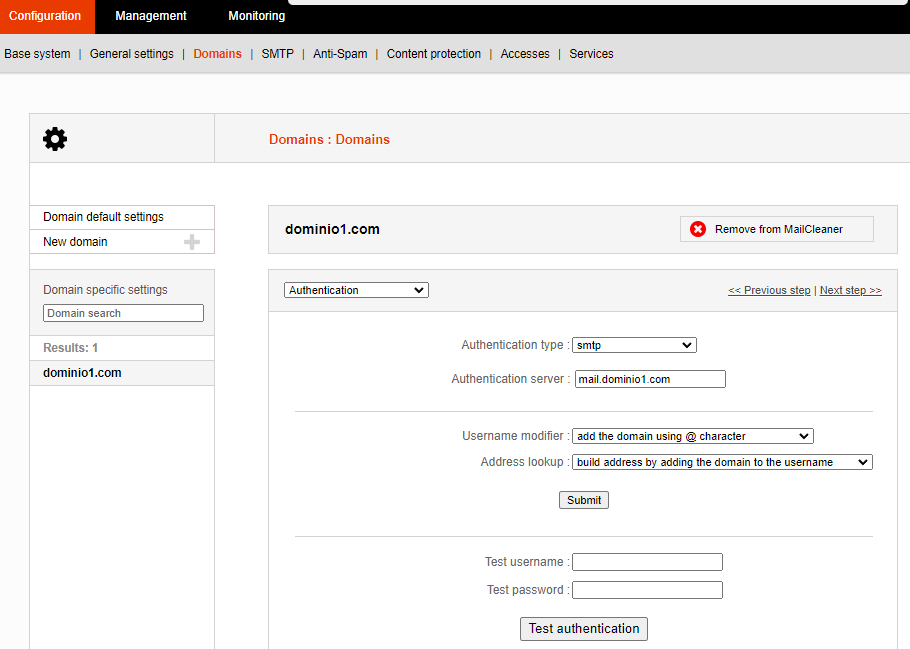




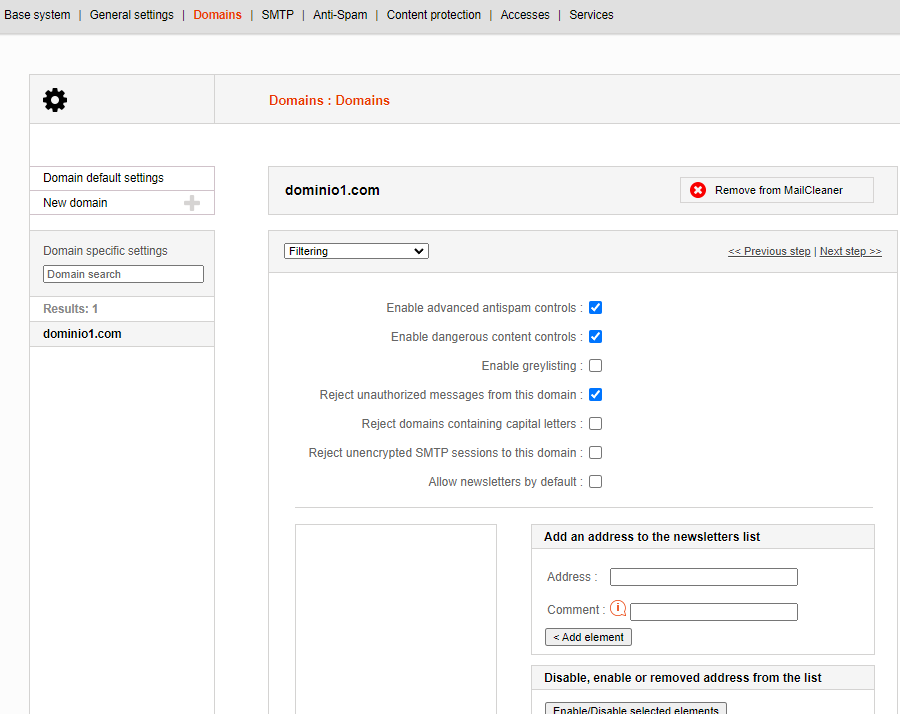
En la siguiente pantalla de configuración elegiremos qué queremos que haga mailclenaner con los mensajes que detecte con virus o spam, las opciones son que solamente los marque con una etiqueta y que los entregue, que los guarde temporalmente como spam en el propio mailcleaner para su posterior análisis o directamente que los rechace



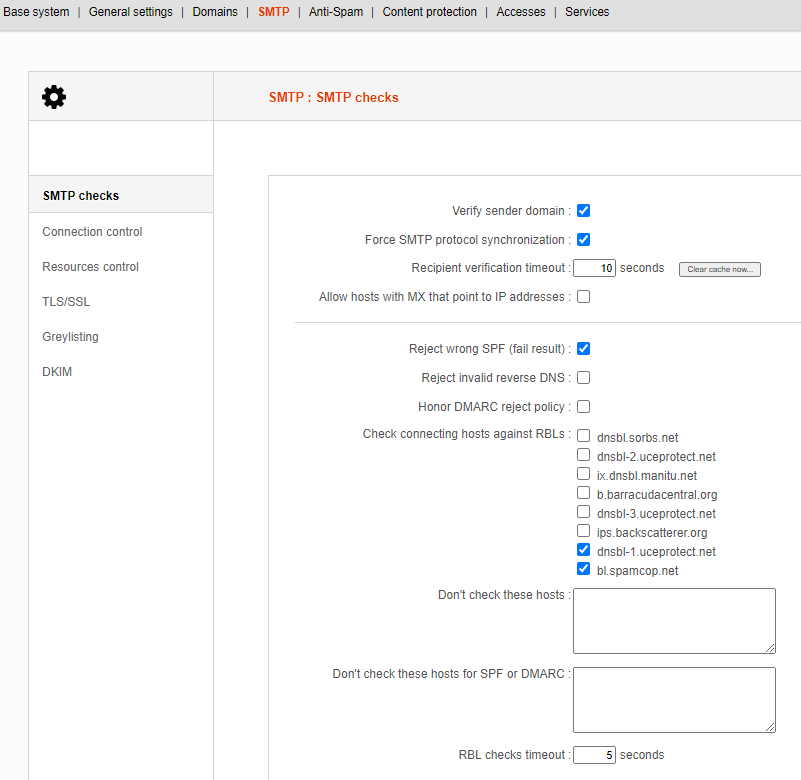
En la pantalla siguiente podremos configurar cómo queremos que mailcleaner loguee a los usuarios en el sistema, de tal forma que un usuario podrá conectar vía web a mailcleaner para ver sus correos que estén bloqueados por spam, etc.



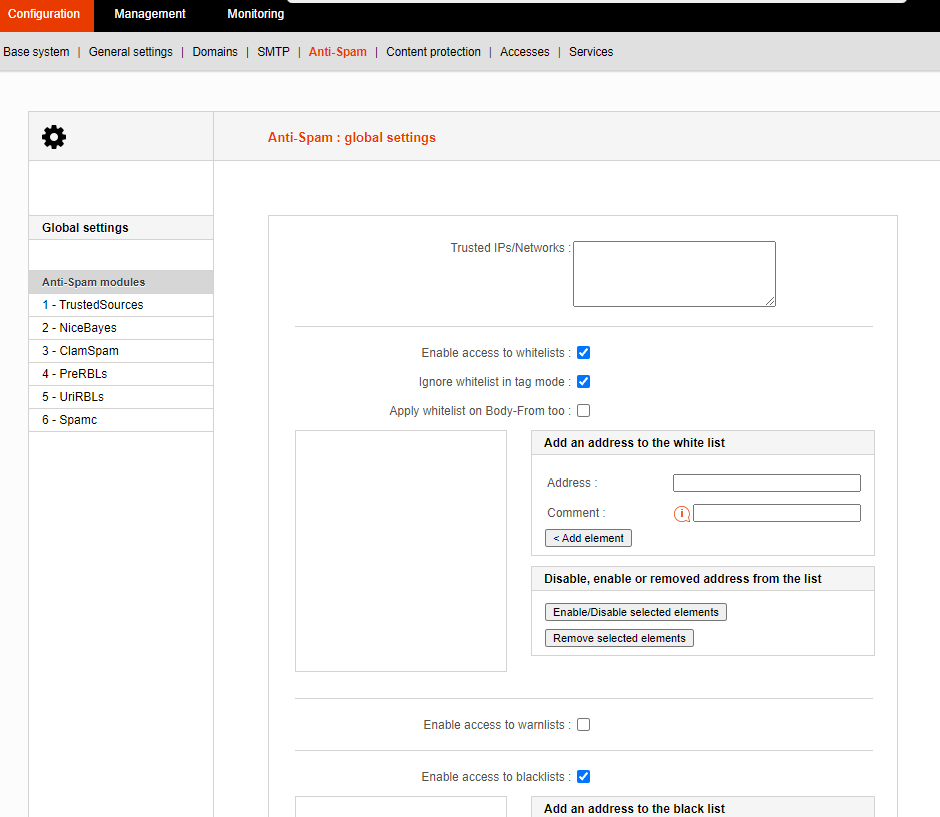
En el siguiente apartado configuraremos el comportamiento del filtrado que se realiza



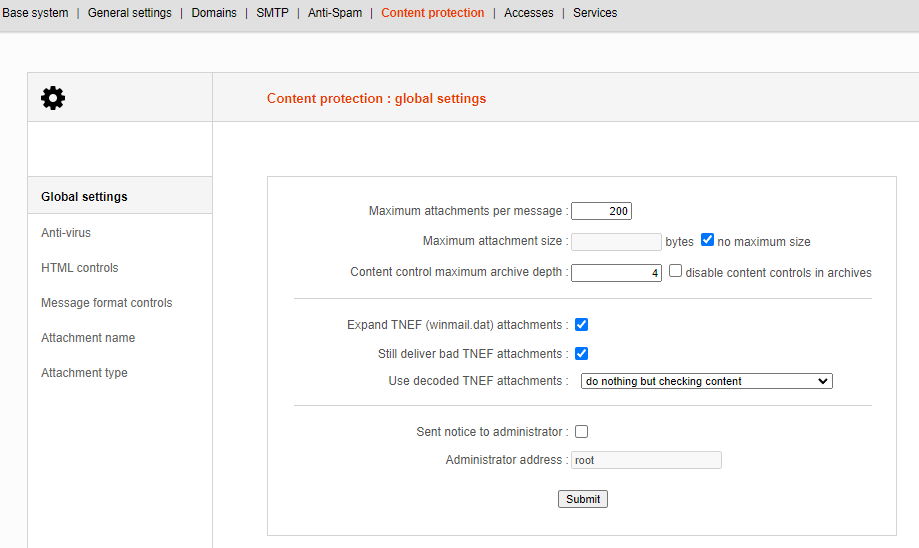
El apartado de la pestaña “SMTP” contiene muchas opciones, algunas de ellas nos permitirán seleccionar listas RBL públicas de internet que contienen direcciones de servidores que son renviadores de spam. Podemos seleccionarlas a nuestro gusto, aunque dejaremos todas las demás opciones por defecto.



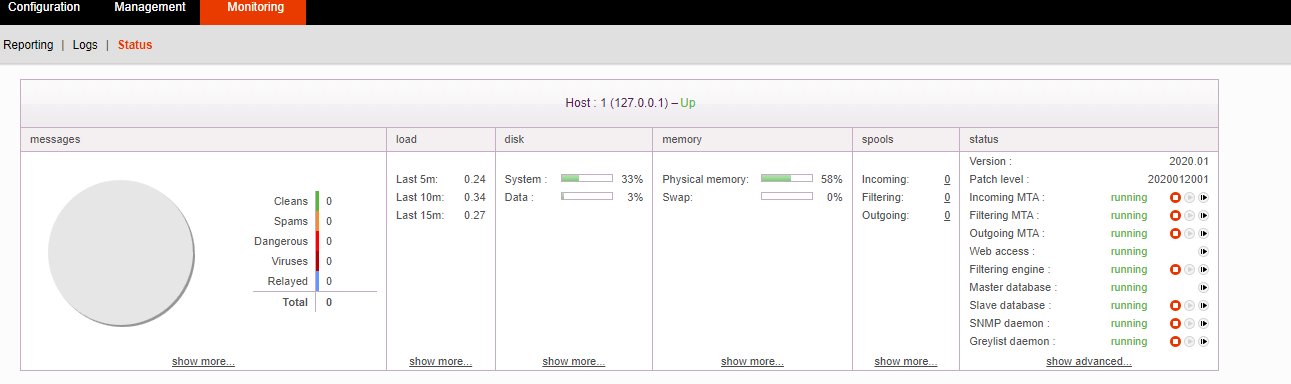
Apartado de la pestaña “Anti-Spam”. Activamos las dos opciones marcadas en amarillo para poder introducir direcciones de email o “cuenta@nombrededominio” o dominios enteros “\*@nombrededominio” en listas blancas o listas negras



En la siguiente pestaña “Content protection” podemos elegir si queremos que bloque correos que lleven cierto tipo de adjuntos como, por ejemplo, ejecutables, zip comprimidos con contraseñas, etc.



Para finalizar tenemos “Monitoring” donde podremos ver los logs del sistema y los servicios de mailcleaner.



Para comprobar el funcionamiento de mailcleaner en nuestros sistemas de pruebas lo tenemos muy difícil ya que, por una parte, el domino que estamos utilizando no existe en internet y por otra parte, las direcciones ips de nuestros servidores son internas y no tienen puertos en escucha desde el exterior.