Guía General de Seguridad para Administración de Servidores de Correos Zimbra

Fecha de publicación: 31/03/2022

TAGS: Zimbra, DNS

Tema: Guía general de seguridad en servidores de correo electrónico Zimbra.

Objetivo: Proveer instrucciones sobre cómo evitar y protegerse contra ataques de SPAM y *mail spoofing* en servidores y clientes de correo electrónico (principalmente Zimbra) para algunos escenarios posibles, con el fin de reducir el potencial riesgo de dichos ataques y evitar que la reputación del sitio sea dañada por atacantes mal intencionados. Así también proveer información sobre SPF, DMARC y DKIM.

Índice

Glosario

Spoofing	Falsificar la dirección de envío de una transmisión (correos, mensajes, etc) para obtener acceso ilegal a un sistema seguro
Spam	Correo electrónico basura, abuso de los sistemas de mensajería electrónica para el envío masivo de mensajes no solicitados
Spammer	Individuo que remite correos spam
Telnet	Protocolo de red que permite acceder a una máquina remota para administrarla, por defecto la comunicación entre la máquina el equipo remoto no posee encriptación, por lo cual es considerado inseguro
Zimbra	Suite de aplicaciones colaborativas (correo electrónico, calendario, contactos y colaboración basada en nube) con interfaz basada en web, distribuida bajo las modalidades opensource y empresariales
vim	Editor de texto, compatible con la mayoría de sistemas UNIX
Webmail	Aplicación de correo electrónico, accesible a través de un navegador web

Acrónimos

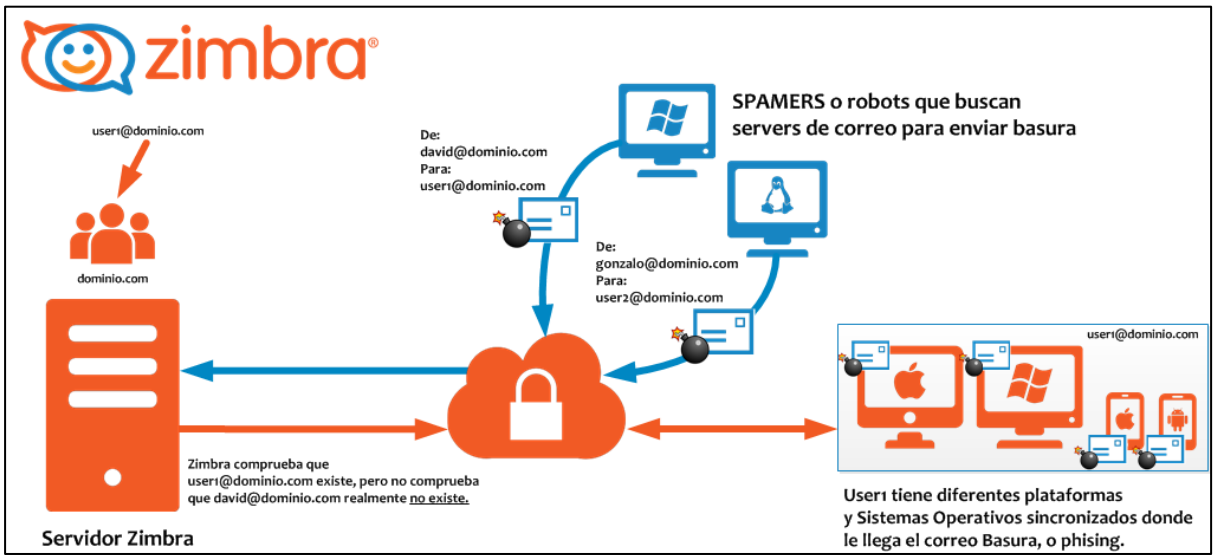
SASL	Simple Authentication and Security Layer
2FA	Double Factor Authentication
MTA	Mail Transfer Agent
RBL	Real-time blackhole list
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DKIM	DomainKeys Identified Mail
SPF	Sender Policy Framework
DNS	Domain Name System
NDR	Non Delivery Receipt
CLI	Command-line interface
ZCO	Zimbra Connector for Outlook
ZCS	Zimbra Community Server

Escenario 1 – Rechazar correos falsos mail "***from***"

Uno de los principales problemas de SPAM se genera al permitir que falsos mail "***from***" envíen correos a los usuarios. De modo que al ejecutar un comando telnet al puerto 25, se podría enviar un correo hacía un usuario legítimo *usuario@dominio.com* desde una cuenta con el mismo dominio como, por ejemplo *usuario2@dominio.com*

Para más información acerca de *Spoofing* ingresar al siguiente enlace.

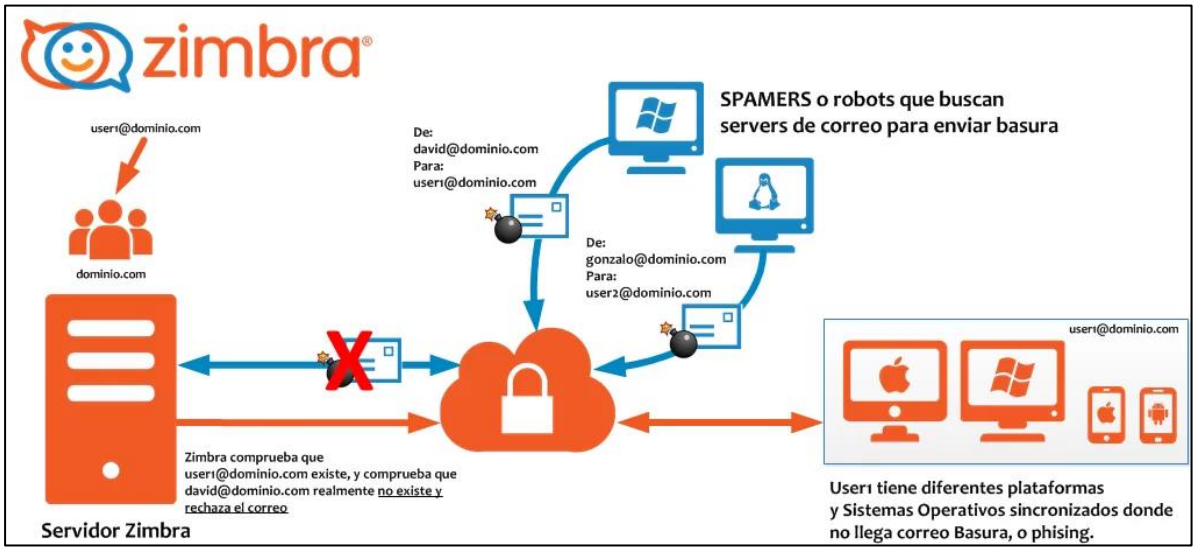
Esquema actual:



Para *ZIMBRA Collaboration 8.5 y superior*, utilice los siguientes comandos para aumentar la seguridad y rechazar estos falsos mail "***from***", ejecutando con el usuario zimbra los siguientes comandos:

```
zmprov mcf zimbraMtaSmtpdRejectUnlistedRecipient yes
zmprov mcf zimbraMtaSmtpdRejectUnlistedSender yes
zmmtactl restart
zmconfigdctl restart
```

Esquema actual luego de la ejecución de los comandos:



Podría realizar una prueba para comprobar la correcta configuración:

```
Equipo:~ usuario$ telnet mail.dominio.com 25
Trying mail.dominio.com...
Connected to mail.dominio.com.
Escape character is '^]'.
220 mail.dominio.com ESMTP Postfix
ehlo mail.dominio.com
250-mail.dominio.com
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

```
mail from: hi@dominio.com
250 2.1.0 Ok
rcpt to: admin@dominio.com
550 5.1.0 <hi@dominio.com>: Sender address rejected: dominio.com
```

Escenario 2 – Comprobar el inicio de sesión de usuario en SASL

Por defecto Zimbra permite que, una vez autenticado un usuario, **pueda enviar emails en nombre de otra dirección de correo (Spoofing)**. Para comprobar que el inicio de usuario del usuario (login) y su dirección de correo corresponden con el SASL, existen una de serie de medidas, 5 pasos en total a tener en cuenta para alcanzar un mayor nivel de seguridad contra estos ataques.

Para más información acerca de *Spoofing* ingresar al siguiente enlace.

Pasos para la restricción:

1. Cambiar al usuario Zimbra y abrir ***smtpd_sender_restrictions.cf*** utilizando el editor *vim*.

```
su - zimbra
vim /opt/zimbra/conf/zmconfigd/smtpd_sender_restrictions.cf
```

2. Agregar esta línea ***check_sasl_access lmdb:/opt/zimbra/conf/sasl_access*** entre "***permit_mynetworks y permit_sasl_authenticated***".

```
permit_mynetworks, reject_sender_login_mismatch
check_sasl_access lmdb:/opt/zimbra/conf/sasl_access_block
permit_sasl_authenticated
```

3. Crear el archivo ***sasl_access_block*** y agregar un usuario que debería restringirse utilizando la autenticación SASL.

```
vim /opt/zimbra/conf/sasl_access_block
```

```
user1@example.com REJECT Sorry, you are not allowed to use SMTP SASL authentication
.
```

4. Guardar el mismo archivo y ejecutar el comando postmap.

```
postmap /opt/zimbra/conf/sasl_access_block
```

5. Vuelva a cargar el servicio de postfix.

```
postfix reload
```

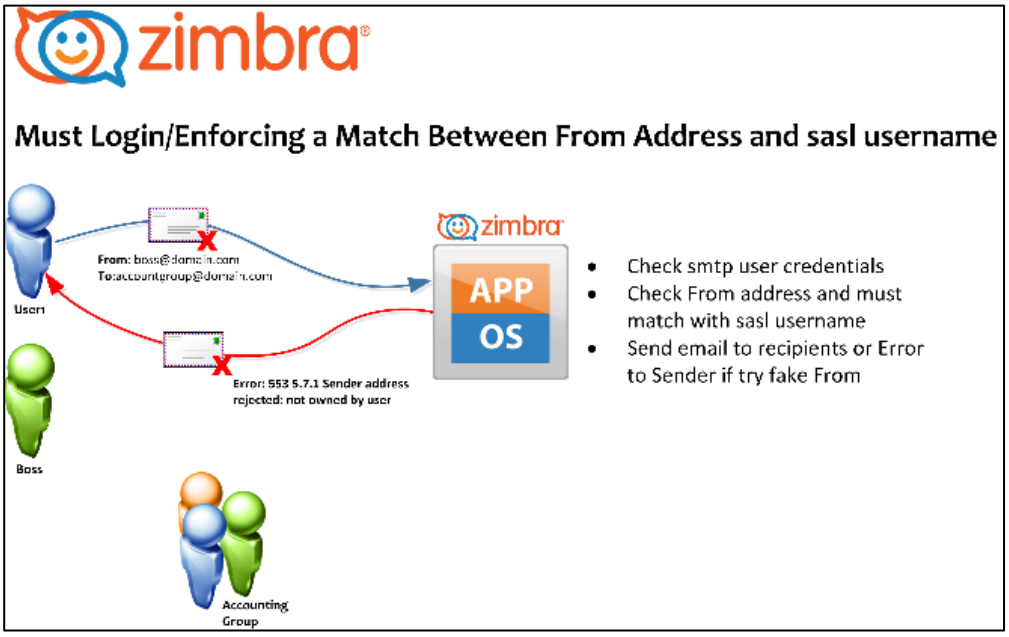
Al finalizar, deberían aparecer las siguientes entradas de registros en ***zimbra.log*** y mostrar un mensaje si un usuario restringido intenta enviar un correo electrónico utilizando la autenticación SASL.

Líneas de registro de ***zimbra.log*****:**

```
Oct 5 14:00:33 proxy postfix/smtps/smtpd[32649]: NOQUEUE: reject: RCPT from unknown[1
72.16.7.222]: 554 5.7.1 <user1@example.com>:

SASL login name rejected: Sorry, you are not allowed to use SMTP SASL authentication.; fr
om=<user1@example.com> to=<user2@example.com> proto=ESMTP helo=<PNQWB7S2
PRKUMA>Rejected
```

El Flujo de Correo queda de la siguiente manera:



OBS: El usuario1 se autentica e intenta enviar un correo usando la dirección de correo de su jefe, pero el sistema Zimbra le devuelve un error al instante.

Escenario 3 – Prevenir el envío de Spoofing interno

Para evitar el envío de spoofing interno, el servidor de correo Zimbra cuenta con el servicio incorporado *SpamAssassin,* evita que, correos electrónicos falsificados con el nombre de "***from***" mediante la habilitación el complemento "*FromNameSpoof; que* predeterminadamente se encuentra deshabilitado. Se debe tener en cuenta la implementación del complemento "*FromNameSpoof*" de *SpamAssassin* se utiliza, para evitar que los *spammers* suplanten direcciones de correo electrónico.

La suplantación de nombre se produce cuando un atacante falsifica el nombre "***from***" de la cabecera del correo electrónico, para que parezca que el correo electrónico ha sido enviado por otra persona, de esta forma los *spammers* falsifican el nombre del remitente.

Para más información acerca de *Spoofing* ingresar al siguiente enlace.

Pasos para realizar la prevención:

1. Habilitar el complemento *FromNameSpoof* descomentando la línea a continuación:

/opt/zimbra/data/spamassassin/localrules/v342.pre

```
loadplugin Mail::SpamAssassin::Plugin::FromNameSpoof
```

2. Descomentar las siguientes líneas y modifique la puntuación de spam según las necesidades:

/opt/zimbra/data/spamassassin/rules/72_active.cf

```
score    T_FROMNAME_EQUALS_TO 1.0
score    T_FROMNAME_SPOOFED_EMAIL 0.3
```

Publicado:

```
ifplugin Mail::SpamAssassin::Plugin::FromNameSpoof
meta     T_FROMNAME_EQUALS_TO __PLUGIN_FROMNAME_EQUALS_TO
describe T_FROMNAME_EQUALS_TO From:name matches To:
score    T_FROMNAME_EQUALS_TO 1.0
tflags   T_FROMNAME_EQUALS_TO publish
endif
```

```
meta     T_FROMNAME_SPOOFED_EMAIL  (__PLUGIN_FROMNAME_SPOOF && !__VIA_ML && !__VIA_RESIGNER && !__RP_MATCHES_RCVD)
describe T_FROMNAME_SPOOFED_EMAIL From:name looks like a spoofed email
score    T_FROMNAME_SPOOFED_EMAIL 0.3
tflags   T_FROMNAME_SPOOFED_EMAIL publish
endif
```

Nota:
T_FROMNAME_EQUALS_TO, esta condición se aplicará cuando el nombre *"**from**"* coincida con la dirección *"**to**"*; es decir:

De Nombre: usuario@dominio.com
Para: usuario@dominio.com
T_FROMNAME_SPOOFED_EMAIL, esta condición se aplicará cuando el nombre del remitente parezca un correo electrónico falsificado; es decir:

De Nombre: usera@domain.com
Desde la dirección: usersome@example.com
Para: usuariob@dominio.com

3. Reiniciar amavid, mta.

```
zmamavisdctl restart
zmmtactl restart
```

Escenario 4 – Prevenir el envío de Spam

Para evitar el envío de correos electrónicos spam, debemos tener en cuenta las siguientes situaciones:

- Una cola de correo extensa provocada por actividad de correos *Spams* entrantes y NDR, puede derivar en denegación del servicio del correo.
- Actividad de *spam* excesiva en el servidor.
- La inclusión en la lista negra de IPs de MTA en los RBL globales tiene un gran impacto en los correos salientes.

Para más información acerca de *SPAM* ingresar al siguiente enlace.

Solución:

La solución se aborda en 2 secciones:

- Reparar
- Prevenir

Reparar:

En esta sección, vemos cómo podemos identificar al *spammer*, controlar el spam y borrar la cola de correos:

- En primer lugar, mantener la cola de correos

```
su - zimbra
~/common/sbin/postsuper -h ALL
```

- Liberar la cola una vez terminado el trabajo

```
~/common/sbin/postsuper -r ALL
```

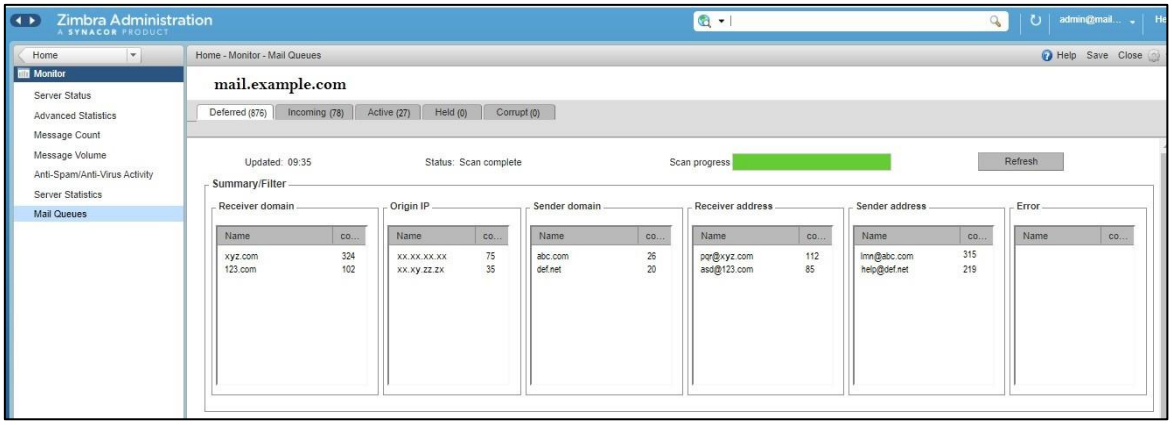
Hay 2 formas de verificar la cola de correo

A) Desde el panel de administración

B) CLI del servidor.

- Primero, verifique la cola de correo desde el Panel de control de administración.

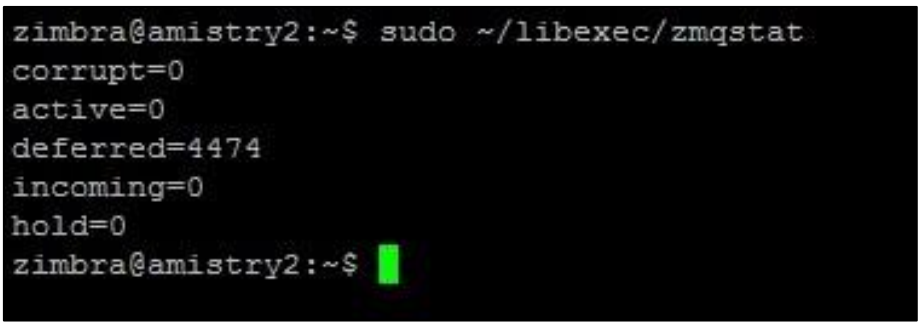
Abra el Panel de administración. Desde el panel izquierdo, vaya a > Monitorear > Colas de correo y la ventana se verá así:



Debido a la carga en el servidor, a veces se vuelve difícil acceder al panel de administración, por lo tanto, verifique el método CLI para encontrar al *spammer*.

Use los siguientes comandos que le darán un resultado casi similar al del panel de administración.

```
$sudo ~/libexec/zmqstat
```



Por lo tanto, al consultar la cola de correo, podemos identificar fácilmente qué dirección de correo electrónico se ha visto comprometida y desde qué direcciones IP se reciben correos no deseados y tomar medidas adicionales.

Prevención*:*

La prevención se ha dividido en 2 secciones

- Nivel de usuario
- Nivel de servidor

1) Precaución a nivel de usuario

(Cuestiones de las que los usuarios finales deben ocuparse)

- Mantener la estación de trabajo libre de infecciones y malware con AS/AV actualizado.
- No acceder a Webmail en PC públicas, ya que la mayoría de ellas están infectadas y el virus puede robar la información de inicio de sesión y proporcionarla al remitente de spam.
- Mantener la contraseña segura, incluya al menos 1 letra mayúscula y 1 letra minúscula, 1 carácter especial y 1 número.
- Cambiar la contraseña con frecuencia, por lo que, si hay alguna fuerza bruta en la cuenta, el script llevará tiempo o no podrá descifrar la contraseña.
- Mantener la estación de trabajo y Outlook actualizados con todos los parches y actualizaciones de seguridad.
- Mantener ZCO actualizado.

- No compartir las credenciales de inicio de sesión con nadie.
- El uso de 2FA será una ventaja adicional.
- No abrir ningún correo electrónico desconocido o archivo adjunto que no haya sido enviado por una fuente confiable.
- Principalmente, no abrir ningún archivo ejecutable como (.exe, .bat, etc.) que podrían ser virus/*malware* que pueden dañar gravemente su sistema.

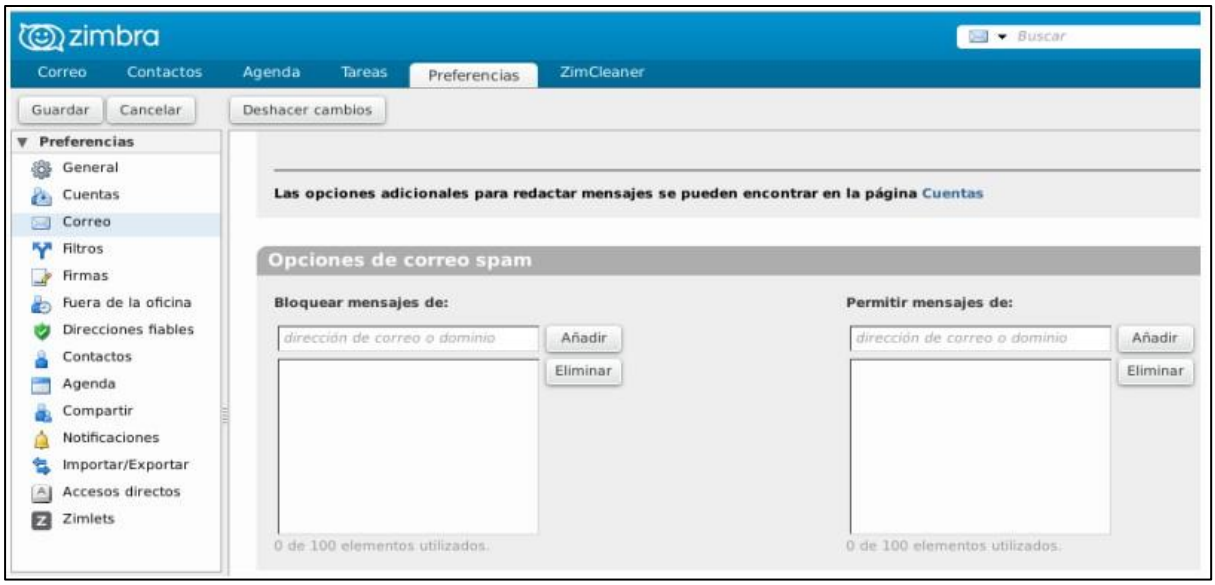
2) Precauciones a nivel de servidor

- Mantener actualizado ZCS a la última versión y parche, ya que incluye todas las actualizaciones relacionadas con el rendimiento y la seguridad que mantendrán el servidor a salvo de ataques importantes.
- Mantener la política de contraseña segura para que los usuarios no puedan establecer una contraseña débil y evitará que se obtenga la contraseña mediante un ataque de fuerza bruta.
- Configurar también la caducidad de la contraseña para que los usuarios no puedan mantener la misma contraseña por mucho tiempo.
- Mantener actualizado el sistema operativo también, porque si hay alguna vulnerabilidad en la versión anterior, también puede afectar el servidor completo ZCS resultante.
- Proteger la red con la ayuda de un ingeniero de redes para que nadie pueda iniciar sesión en el servidor y cambiar la contraseña del administrador o de cualquier usuario para enviar más spam.

Escenario 5 – Administración de listas blancas (whitelist) y negras (blackList)

Existe la posibilidad de administrar del lado del cliente las listas blancas utilizadas para señalar que los correos pertenecientes a dicha lista son de confianza y listas negras utilizadas para indicar que los correos pertenecientes a esa lista no son de confianza. El objetivo es poder administrar los correos y calificarlos según el nivel de confianza que se posea en los remitentes de estos. Su configuración puede realizarse desde las preferencias del usuario. Dicha opción se encuentra ubicado bajo el menú:

Preferencias -> Correo -> Opciones de correo spam:



Creación de registros SPF, DKIM y DMARC

Para configurar los ajustes de autenticación SPF, DKIM y DMARC para tu dominio, es necesario que tenga acceso a los registros DNS de tu sistema de correo electrónico.

Configurar un registro DNS para la autenticación SPF

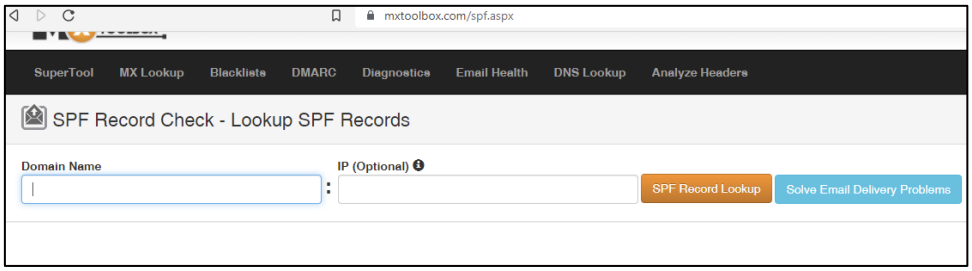
A la hora de llevar a cabo la configuración, debe tener en cuenta dos posibles situaciones sobre de los registros SPF:

● Un registro SPF es un tipo de registro TXT – no debe confundirse con el tipo SPF (utilizable, pero no recomendado para efectos de esta guía).

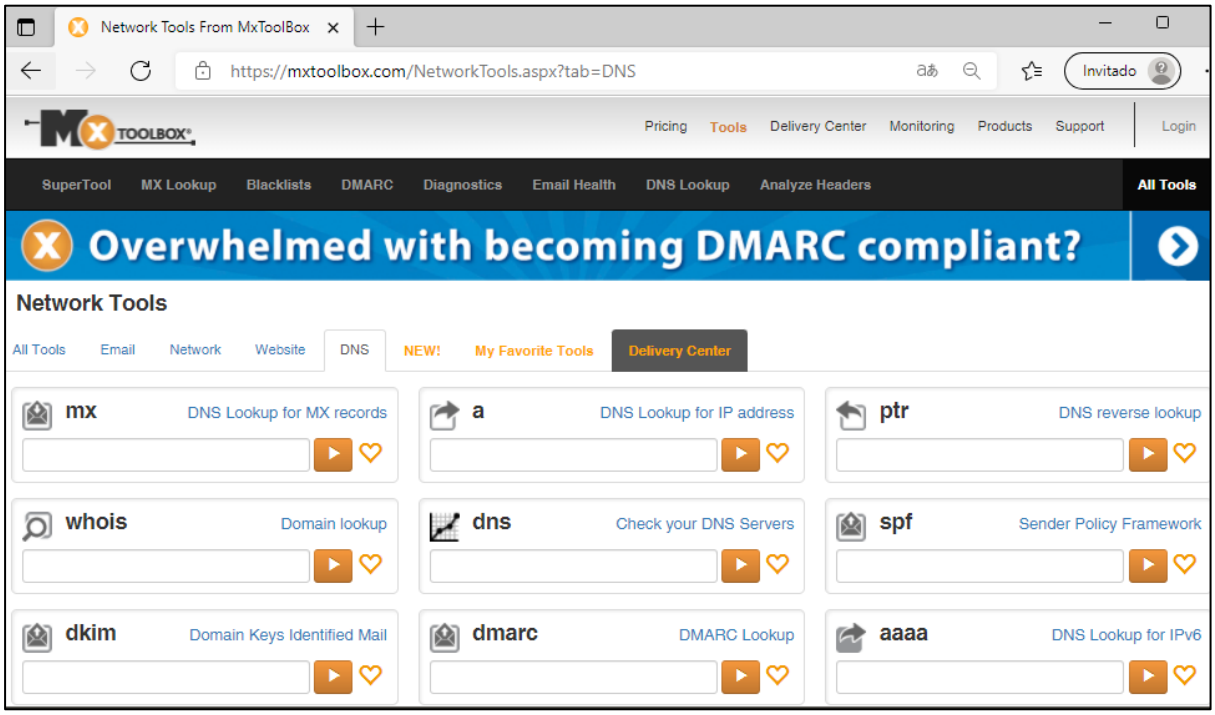
● Sólo debería haber un registro SPF por dominio. Si tienes varios registros DNS SPF, los operadores de email no sabrán cuál usar, lo que podría causar problemas de autentificación.

El SPF se configura a nivel de DNS público del dominio. Si no se visualiza ningún registro SPF, se debe crear uno. De lo contrario, solo se tiene que actualizar el registro SPF existente.

Una herramienta que podría utilizarse para verificar dichos registros, es la web https://mxtoolbox.com/, la misma cuenta con una serie de opciones para verificar los registros de servidores y DNS. Para ello se debe realizar los siguientes pasos:



1. Dirigirse a todas las herramientas “All Tools”.
2. Seleccionar la opción DNS, luego consultar el registro SPF a través, de la opción SPF, provea el valor del dominio que desee consultar el registro.-



El registro SPF requiere de la configuración de una serie de parámetros, en el siguiente ejemplo se muestra como enlazar *office365* y *mailchimp.*

El valor del registro SPF sería:

v=spf1 mx ip4:190.52.XXX.XXX a:xyz.mitic.gov.py include:spf.protection.outlook.com include:spf.mandrillapp.com -all

Con el código anterior, se permitiría enviar correos autorizados por el dominio Web desde las aplicaciones de *office365* y *mailchimp*.

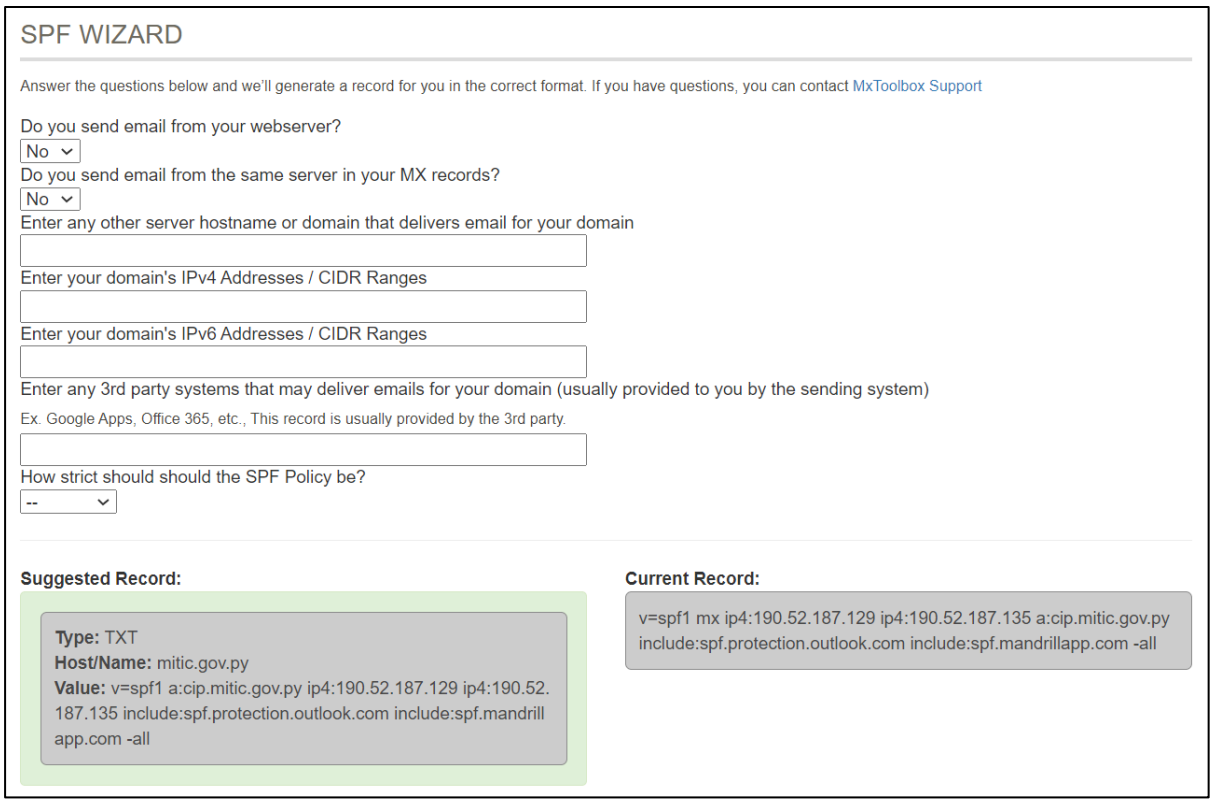
Si además se necesita agregar alguna otra IP autorizada, debe ser incluida en este mismo código, así sucesivamente con todas las autorizaciones que se deba conceder.

También, se podría añadir direcciones IP autorizadas, agregándolas directamente a este mismo código. Por ejemplo, lo comentado anteriormente referenciaría a una aplicación de gestión comercial, desde donde se envían correos automáticos en nombre de una empresa teniendo la dirección IP como la siguiente: 190.52.XXX.XXX

El código TXT pasaría a ser:

v=spf1 ip4:190.52.XXX.XXX include:spf.protection.outlook.com -all

El administrador del dominio, puede generar el código utilizando las siguientes aplicaciones en línea: SPF Record Generator - MxToolBox y https://www.spfwizard.net/ en este caso se muestra la herramienta de *Mxtoolbox* para el dominio **mitic.gov.py**.



Una vez proveídos los campos solicitados, en la sección inferior de la pantalla se podrá visualizar el registro final, este debe ser insertado como un registro TXT en el servidor de DNS público autoritativo del servicio de correo electrónico.

Configurar DKIM

DomainKeys Identified Mail (DKIM) es un mecanismo de autenticación de correo electrónico que permite a una organización responsabilizarse del envío de un mensaje, de manera que éste pueda ser validado por un destinatario

DKIM utiliza criptografía de clave pública para permitir al origen firmar electrónicamente correos electrónicos legítimos de manera que puedan ser verificados por los destinatarios.

DKIM también protege contra la manipulación de correo electrónico, proporcionando integridad de extremo a extremo, desde un módulo firmante a un módulo validador. En la mayoría de los casos el módulo firmante actúa en nombre de la organización originaria

insertando una firma DKIM en las cabeceras del mensaje, y el módulo de comprobación en nombre de la organización del receptor, validando la firma obteniendo la clave pública del firmante a través del DNS. La clave publica de DKIM debe ser generado por su servidor de correo electrónico, y configurado en forma de registro en su servidor de DNS público.

Para la creación de la clave del DKIM en un servidor de correo electrónico, podría seguirse la siguiente documentación para los servidores de correo más implementados:

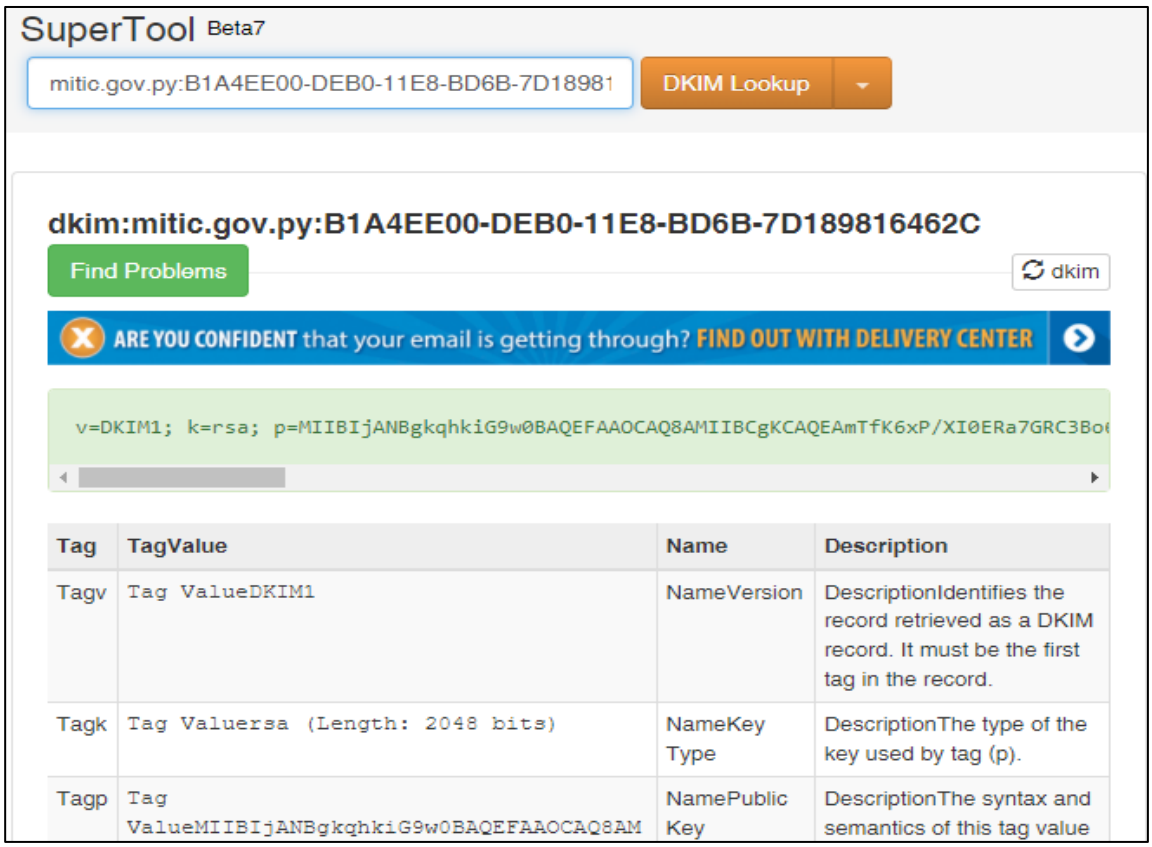
- Zimbra: http://wiki.zimbra.com/wiki/Configuring_for_DKIM_Signing
- Microsoft Exchange: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dkim-to-validate-outbound-email?view=o365-worldwide

Con el DKIM generado desde el servidor de correo, debe ser insertado en su registro de DNS público en formato registro o TXT, utilizando el siguiente formato (v=(versión), k=(Tipo de clave), P(Clave Publica), puede utilizar un generador de registro DKIM, proveyendo los registros de selector y dominio

- https://easydmarc.com/tools/dkim-record-generator

Una vez cargado el registro en el servidor de DNS, puede consultar dicho registro utilizando la herramienta en línea:

- https://mxtoolbox.com/dkim.aspx



Configurar DMARC

Mecanismo de autenticación de correo electrónico, diseñado para otorgar a los propietarios de dominios de correo electrónico la capacidad de proteger su dominio frente a su uso no autorizado, comúnmente conocido como email spoofing. El propósito principal de implementar DMARC, es proteger el dominio de la organización, contra ataques que comprometan el correo electrónico de las empresas, el envío de correos electrónicos de phishing, spam y otras ciber amenazas.

Una vez publicada la entrada DNS de DMARC, cualquier servidor receptor de correos electrónicos puede autenticar el mensaje entrante de correo electrónico conforme a las instrucciones publicadas por el propietario del dominio dentro de la entrada DNS.

DMARC amplía el funcionamiento de dos mecanismos de autenticación existentes, Sender Policy Framework (SPF) y DomainKeys Identified Mail (DKIM). Permitiendo al propietario administrativo de un dominio publicar una política en sus registros DNS que indica qué mecanismo (DKIM, SPF o ambos) se emplea durante el envío de los mensajes de correo electrónico desde ese dominio.

Antes de implementar DMARC se debe verificar que los registros SPF y DKIM hayan sido implementados correctamente. DMARC define cuál es la política por aplicar en caso de fallo en los protocolos SPF y DKIM, a través de un registro DNS dedicado.

DMARC le permite aplicar una de estas tres políticas, en caso de no correspondencia:

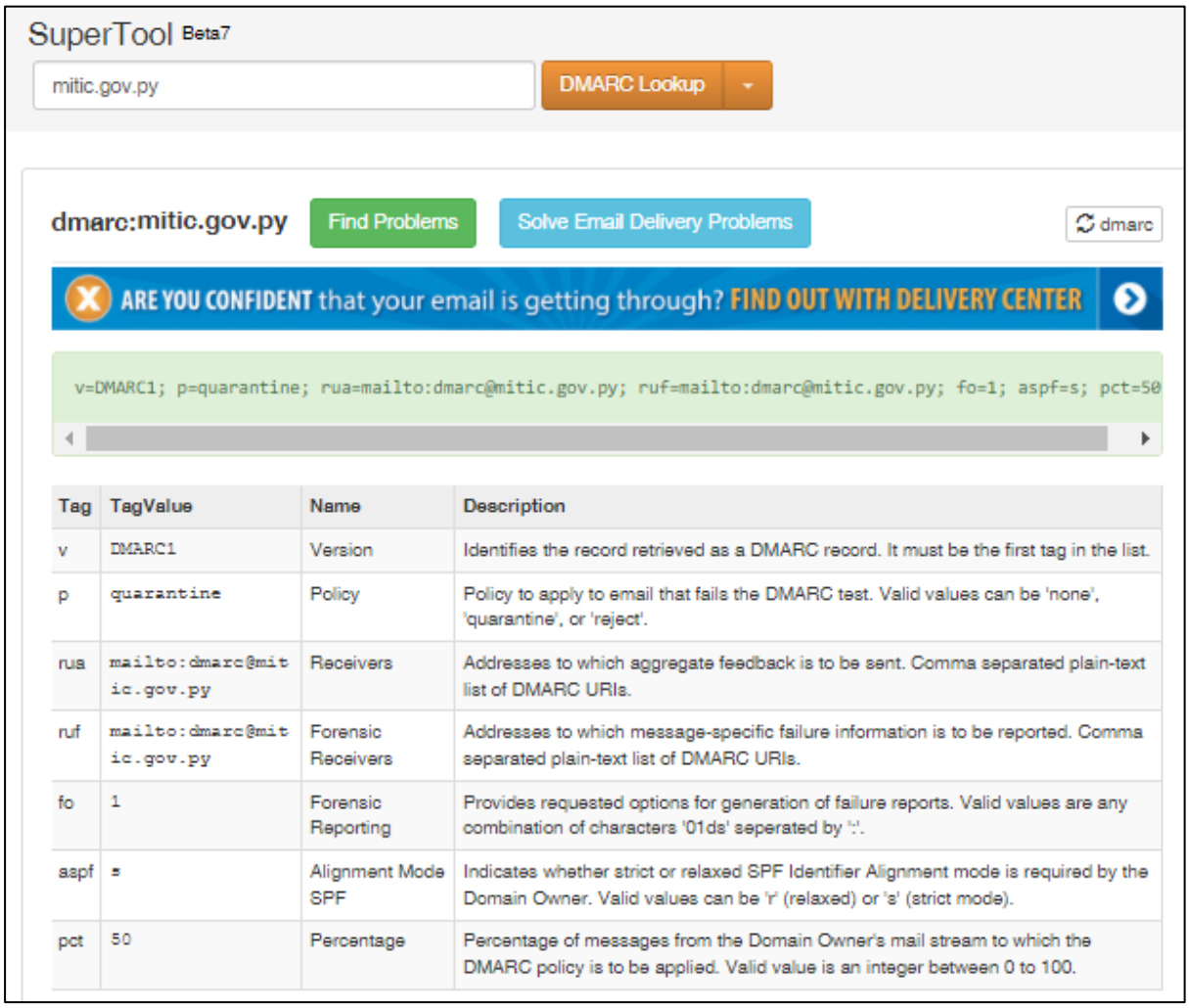
1. **Ninguna**: ninguna acción, aplicar la política local.
2. **Cuarentena**: marcado como spam.
3. **Rechazar**: rechazar el mensaje.

El registro DMARC es otro registro de tipo TXT, este se configura en el servidor de DNS público del dominio. Este es un protocolo instructivo, que especifica cómo manejar los registros SPF y DKIM, y el valor del registro TXT con el que debes configurar tu registro DMARC sería como:

v=DMARC1; p=quarantine; mitic.gov.py; mitic.gov.py; fo=1; aspf=s; pct=50

Los informes XML que genere DMARC, serán enviados a la dirección configurada en el parámetro “rua=”. Aquí se podrá encontrar toda la información sobre los correos que han sido enviados bajo el dominio registrado, controlando si ha existido violación a los protocolos de seguridad con la posibilidad de conocer cuales protocolos han sido violados. Estos datos son considerados de gran utilidad debido a que ayudarían a descifrar todos los intentos de suplantación y estafa que podrían haberse cometido utilizando el nombre de una empresa particular.

Podría usar la siguiente herramienta en línea para generar el registro DMARC Record Generator - Create DMARC DNS Records - MxToolbox a continuación, se muestra una lista de los valores que podrían configurarse en el protocolo y que debería tener en cuenta:



Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	quarantine	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
rua	mailto:dmarc@mitic.gov.py	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.
ruf	mailto:dmarc@mitic.gov.py	Forensic Receivers	Addresses to which message-specific failure information is to be reported. Comma separated plain-text list of DMARC URIs.
fo	1	Forensic Reporting	Provides requested options for generation of failure reports. Valid values are any combination of characters '01ds' seperated by ':'.
aspf	s	Alignment Mode SPF	Indicates whether strict or relaxed SPF Identifier Alignment mode is required by the Domain Owner. Valid values can be 'r' (relaxed) or 's' (strict mode).
pct	50	Percentage	Percentage of messages from the Domain Owner's mail stream to which the DMARC policy is to be applied. Valid value is an integer between 0 to 100.

Puede usar la siguiente herramienta en línea para generar el registro DMARC Record Generator - Create DMARC DNS Records - MxToolbox a continuación, listamos los valores utilizados frecuentemente que pueden ingresarse en el registro.

El registro DMARC

La política DMARC es codificada en un registro TXT alojado en el DNS del dominio remitente. Similar al registro SPF y DKIM, la política DMARC es codificada bajo una serie de valores tag=valor

Tag	Nombre	Descripción
v=	Versión	Campo de versión que debe estar presente como primer elemento. De forma predeterminada el valor es DMARC1.
p=	Política	Campo de política obligatorio. Puede tomar valor ninguno, cuarentena o rechazar. Esto permite una política de endurecimiento gradual en la que el dominio del remitente no recomienda ninguna acción específica en el correo que no supere las comprobaciones de DMARC. (p = ninguno) considerando el correo fallido como sospechoso (p = cuarentena) para rechazar todo el correo fallido (p = rechazar) preferiblemente en la etapa de transacción SMTP.
aspf=	Política SPF	El valor "r" (predeterminado) significa relajado El valor "s" requiere una coincidencia exacta entre el dominio del Mensaje-De: dirección y la verificación SPF (aprobada) debe coincidir exactamente con el sobre RFC-De: dirección (es decir, la dirección: HELO). *Relaxed* requiere que solo los dominios de dirección mensaje-De: y remitente estén alineados. Por ejemplo, la remitente dirección parte de dominio "smtp.example.org" y el mensaje-De: dirección "anuncio@example.org" están alineados, pero no son una coincidencia estricta.
fo=	Opciones de fallo de reportes	Es opcional. Ignore si un argumento "ruf" a continuación no está presente también. El valor 0 indica que el receptor debe generar un informe de falla DMARC si todos los mecanismos subyacentes fallan en producir un resultado de "aprobación" alineado. El valor 1 significa generar un informe de falla de DMARC si cualquier mecanismo subyacente produce algo diferente a un resultado de "aprobado" alineado. Otros valores posibles son “d” y “s”: “d” significa generar un informe de falla de DKIM si una firma falla en la evaluación. “S” significa generar un informe de falla de SPF si el mensaje no pasó la evaluación de SPF. Estos valores no son exclusivos y pueden combinarse en una lista separada por dos puntos.
ruf=		Es parámetro es opcional. Enumera una serie de Indicadores de recursos universales (URI) (actualmente solo "mailto: <emailaddress>") que enumeran dónde enviar informes de retroalimentación de fallas. Es para informes sobre fallas específicas de mensajes. Los propietarios de dominios de envío deben usar este

		argumento con moderación, ya que se usa para solicitar un informe por falla, lo que podría resultar en un gran volumen de informes de fallas.
rua=		Lista opcional de URI (como en ruf = anterior, usando la lista "mailto:" URI) se utiliza para enviar comentarios agregados al propietario del dominio remitente. Estos informes se envían en función del intervalo solicitado mediante la opción "ri =" a continuación, con un valor predeterminado de 86400 segundos si no aparece en la lista.
ri=	Intervalo de Respuesta	Opcional con el valor predeterminado de 86400 segundos (un día). El valor indicado es el intervalo de informe deseado por el propietario del dominio remitente.
pct=	Porcentaje	Opcional con el valor predeterminado de 100 (%). Expresa el porcentaje de correo del propietario de un dominio que envía que debe estar sujeto a la política DMARC dada en un rango de 0 a 100. Esto permite a los propietarios de dominios aumentar la aplicación de sus políticas gradualmente y evitar tener que comprometerse con una política rigurosa antes de recibir comentarios. en su política existente. Nota: este valor debe ser un número entero.
sp=	Política de Subdominio	Opcional con un valor predeterminado de ninguno. Otros valores incluyen el mismo rango de valores que el argumento "p =". Esta es la política que se aplicará al correo de todos los subdominios identificados del DMARC RR dado. Si un receptor no encuentra un RR DMARC válido para un dominio de envío dado, intentará encontrar un RR DMARC para una zona principal y aplicará una política DMARC si la etiqueta sp = está presente.

Una vez generado este registro, debe ser insertado en el servidor de DNS del dominio para el sistema de correo electrónico que se busca proteger.
Si usted no posee la administración sobre sus registros DNS, una vez generados los valores DKIM, SPF y DMARC para el dominio de correo electrónico, debe solicitar al administrador de su servicio de DNS la creación de dichos registros.

OBS: Tener en cuenta que el uso correcto de DMARC es arbitrario, y queda a criterio de la postura de ciberseguridad que tenga instaurada la organización, tome los recaudos necesarios para evitar un mal funcionamiento o rebotes de correos electrónicos inesperados.

Referencias:

- https://wiki.zimbra.com/wiki/How-to-restrict-ssl-login
- https://wiki.zimbra.com/wiki/Enforcing_a_match_between_FROM_address_and_sasl_username_8.5
- https://wiki.zimbra.com/wiki/FromName_Spoofing
- https://wiki.zimbra.com/wiki/Preventing_Spamming
- https://www.jorgedelacruz.es/2014/04/03/zimbra-seguridad-i-parte/
- https://www.jorgedelacruz.es/2014/09/08/zimbra-seguridad-ii-parte-enforcing-a-match-between-from-address-and-sasl-username-en-zimbra-8-5/
- https://www.jorgedelacruz.es/2015/07/21/zimbra-seguridad-iii-parte/
- https://www.cert.gov.py/application/files/3914/1685/0242/AntiSpam_para_Zimbra.pdf
- https://blog.zimbra.com/2015/04/email-protection-best-practices-spf-dkim-dmarc/
- https://csrc.nist.gov/glossary