Práctica recomendada para la autenticación de correo electrónico: formas óptimas de implementar SPF, DKIM y DMARC

Contenido

Introducción

Esta guía describe tres tecnologías de autenticación de correo electrónico predominantes que se utilizan actualmente: SPF, DKIM y DMARC, y analiza diversos aspectos de su implementación. Se abordan varias situaciones de arquitectura de correo electrónico en la vida real, así como directrices para implementarlas en el conjunto de productos Cisco Email Security. Puesto que se trata de una guía práctica de prácticas recomendadas, se omitirán algunos de los materiales más complejos. Cuando sea necesario, algunos conceptos pueden simplificarse o condensarse para facilitar la comprensión de la cuestión presentada.

Requisitos de conocimiento del producto

Esta guía es un documento de nivel avanzado. Para continuar con el material presentado, el lector debe poseer conocimientos sobre el producto de Cisco Email Security Appliance hasta el nivel de certificación de Cisco Email Security Field Engineer. Además, los lectores deben tener un fuerte comando de DNS y SMTP y su funcionamiento. El conocimiento de los fundamentos de SPF, DKIM y DMARC es una ventaja.

Autenticación de correo electrónico: breve descripción

Marco de políticas de remitente (SPF)

El marco de políticas de remitente se publicó por primera vez en 2006, como RFC4408. La versión actual se especifica en RFC7208 y se actualiza en RFC7372. Básicamente, proporciona una forma sencilla para que un propietario de dominio anuncie sus orígenes de correo electrónico legítimos a los receptores mediante DNS. Aunque SPF autentica principalmente la dirección de ruta de retorno (MAIL FROM), la especificación recomienda (y proporciona un mecanismo) también autenticar el argumento SMTP HELO/EHLO (FQDN del gateway del remitente tal como se transmitió durante la conversación SMTP).

SPF utiliza registros de recursos DNS de tipo TXT con una sintaxis bastante simple:

```
spirit.com       texto = "v=spf1 mx a ip4:38.103.84.0/24 a:mx3.Spiri.com
a:mx4.Spiri.com incluir:spf.protection.outlook.com ~all"
```

El registro de Spirit Airlines anterior permite que el correo electrónico de las direcciones @Spirit.com provenga de una subred /24 en particular, dos máquinas identificadas por un FQDN y el entorno Office365 de Microsoft. El calificador "~all" al final indica a los receptores que consideren cualquier otra fuente como Soft Fail - uno de los dos modos de falla de SPF. Tenga en cuenta que los remitentes no especifican qué deben hacer los receptores con los mensajes fallidos, hasta qué punto fallarán.

Delta, por otro lado, emplea un esquema diferente de SPF:

```
delta.com texto = "v=spf1 a:smtp.hosts.delta.com
incluir:_spf.proveedor.delta.com -all"
```

Para minimizar el número de consultas de DNS necesarias, Delta creó un único registro "A" que enumera todas sus gateways SMTP. También proporcionan un registro SPF independiente para sus proveedores en "_spf.Vendor.delta.com". También incluyen instrucciones para **Falla Dura** cualquier mensaje no autenticado por SPF ("-all" cualifier). Podemos buscar más a fondo el registro SPF de los proveedores:

```
_spf.Vendor.delta.com texto = "v=spf1 incluir:_spf-delta.vrli.com
incluir:_spf-ncr.delta.com a:delta-spf.niceondemand.com
incluir:_spf.airfrance.fr incluir:_spf.qemailserver.com
incluir:skytel.com incluir:epsl1.com all"
```

Por lo tanto, los correos electrónicos de los remitentes @delta.com pueden provenir legítimamente, por ejemplo, de los gateways de correo electrónico de Air France.

United, por otro lado, utiliza un esquema de SPF mucho más simple:

```
texto de united.com = "v=spf1 incluir:spf.enviaremails.com.br
incluir:spf.usa.net incluir:coair.com ip4:161.215.0.0/16
ip4:209.87.112.0/20 ip4:74.112.71.93 ip4:74.209.251.0/24 mx ~all"
```

Además de sus propios gateways de correo electrónico corporativos, incluyen sus proveedores de marketing de correo electrónico ("usa.net" y "enviaremails.com.br"), gateways de Continental Air Lines heredados, así como todo lo que aparece en sus registros MX ("mecanismo MX"). Tenga en cuenta que MX (un gateway de correo **entrante** para un dominio) puede no ser el mismo que **saliente**. Aunque para las empresas más pequeñas suelen ser las mismas, las organizaciones de mayor tamaño dispondrán de una infraestructura independiente que gestiona el correo entrante y gestiona por separado la entrega saliente.

Además, cabe destacar que todos los ejemplos anteriores hacen un uso extensivo de referencias DNS adicionales ("incluir" mecanismos). Sin embargo, debido a razones de rendimiento, la especificación SPF limita el número total de búsquedas DNS necesarias para recuperar un registro final a **diez**. Cualquier búsqueda SPF con más de 10 niveles de recursión DNS fallará.

Correo identificado con claves de dominio (DKIM)

DKIM, especificado en los RFC 5585, 6376 y 5863 es una combinación de dos propuestas históricas: DomainKeys de Yahoo y Internet Mail de Cisco. Proporciona una forma sencilla de que los remitentes firmen criptográficamente los mensajes salientes e incluyan las firmas (junto con otros metadatos de verificación) en un encabezado de correo electrónico ("DKIM-Signature"). Los remitentes publican su clave pública en el DNS, lo que facilita que cualquier receptor recupere la clave y verifique las firmas. DKIM no autentica el origen de los mensajes físicos, sino que se basa en el hecho de que si el origen está en posesión de la clave privada de la organización remitente, está implícitamente autorizado a enviar un correo electrónico en su nombre.

Para implementar DKIM, la organización de envío generaría uno o más pares de claves públicas y publicaría las claves públicas en el DNS como registros TXT. Un "selector" haría referencia a cada par de claves para que los verificadores DKIM puedan diferenciar entre claves. Se firmarían los mensajes salientes y se insertaba el encabezado DKIM-Signature:

```
Firma DKIM: v=1; a=rsa-sha1; c=relajado/relajado; s=unidos;
d=news.united.com;h=MIME-Version:Content-Type:Content-Transfer-
Encoding:Fecha:A:De:Responder-A:Asunto:Lista-Cancelar-
suscripción:Message-ID; i=MileagePlus@news.united.com;
bh=IBSWR4yzI1PSRYtWLx4SRDSWII4=;

b=HrN5QINgnXwqkx+Zc/9VZys+yhikrP6wSZVu35KA0jfgYzhzSdfA2nA8D2JYIFTNLO8j4D
GmKhH1MMTyYgwYqT0
1rEwL0V8MEY1MzxTrzijkLPGqt/sK1WZt9pBacEw1fMWRQLf3BxZ3jaYtLoJMRwxtgoWdfHU
35CsFG2CNYLo=
```

El formato de la firma es bastante sencillo. "a" especifica los algoritmos utilizados para la firma, "c" especifica los esquemas de canonicalización utilizados [1], "s" es el selector o referencia de clave, "d" es el dominio de firma. El resto de este encabezado DKIM-Signature es específico del mensaje: "h" enumera los encabezados firmados, "i" enumera la identidad del usuario firmante y, finalmente, el encabezado finaliza con dos hashes separados: "bh" es un hash de encabezados firmados, mientras que "b" es el valor hash para el cuerpo del mensaje.

Al recibir un mensaje firmado por DKIM, el receptor buscará la clave pública mediante la siguiente consulta DNS:

```
<selector>._domainkey.<dominio de firmas>
```

según lo especificado en el encabezado DKIM-Signature. Para el ejemplo anterior, nuestra consulta sería "united._domainkey.news.united.com":

```
united._domainkey.news.united.com texto = "g=*\; k=rsa\; n=" "Contactar"
"postmaster@responsys.com" "con" "cualquier" "preguntas" "relativas" "a"
"esta" "firma "\;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/Vh/xq+sSRLhL5CRU1drFTGMXX/Q2Kk
Wgl35hO4v6dTy5Qmxcuv5Awqx
Liz9d0jBaxtuvYALjlGkxmk5MemgAOcCr97GlW7Cr11eLn87qdTmyE5LevnTXxVDMjIfQJt6
OFzmw6Tp1t05NPW h0PbyUohZYt4qpcbiz9Kc3UB2IBwIDAQAB\;"
```

El registro DNS devuelto contiene la clave, así como otros parámetros opcionales. [2]

El problema principal con DKIM es que la especificación inicial no permitía la publicidad que un remitente utiliza DKIM. Por lo tanto, si un mensaje se produce sin una firma, no es fácil para un receptor saber que debería haberse firmado y que, en ese caso, lo más probable es que no sea auténtico. Dado que una sola organización puede utilizar (y lo más frecuente lo hará) varios selectores, no es trivial "adivinar" si un dominio está habilitado para DKIM. Se desarrolló una norma separada, Author Domain Signing Practices, para cubrir esto, pero debido al bajo uso y a otros problemas, en 2013 quedó obsoleta sin sucesor.

Autenticación, Informes Y Conformidad De Mensajes Basados En Dominio (DMARC)

DMARC es la más joven de las tres tecnologías de autenticación de correo electrónico cubiertas y se desarrolló específicamente para abordar las deficiencias de SPF y DKIM. A diferencia de los otros dos, autentica el encabezado de un mensaje y enlaza las comprobaciones realizadas anteriormente por los otros dos. DMARC se especifica en RFC7489.

El valor añadido de DMARC sobre SPF y DKIM incluye:

- Asegurarse de que todas las identidades disponibles (HELO, MAIL FROM y/o dominio de firmas DKIM) estén alineadas (exactamente coincidentes o subordinadas) con el encabezado From
- Proporcionar un medio para que el propietario del dominio del remitente especifique una política para los receptores sobre cómo **deben** manejar los mensajes fallidos
- Proporcionar a los propietarios de dominios de remitentes un servicio de comentarios para que sean informados de cualquier mensaje fallido, facilitando así la identificación de campañas de suplantación de identidad o errores en la asignación de políticas SPF/DKIM/DMARC

DMARC también utiliza un simple mecanismo de distribución de políticas basado en DNS:

```
_dmarc.aa.com texto = "v=DMARC1\; p=ninguno\; fo=1\; ri=3600\;
rua=mailto:american@rua.agari.com,mailto:dmarc@aa.com\;
ruf=mailto:american@ruf.agari.com,mailto:dmarc@aa.com"
```

La única etiqueta obligatoria en la especificación de política de DMARC es "p", especificando la política que se debe utilizar en los mensajes con errores. Puede ser uno de los tres: ninguno, cuarentena, rechazar.

Los parámetros opcionales más utilizados tienen que ver con la generación de informes: "rua" especifica una URL (ya sea un mailto: o una URL http:// mediante el método POST) para enviar informes agregados diarios de todos los mensajes fallidos que pretendan provenir de un dominio determinado. "ruf" especifica una URL para enviar informes detallados de fallos inmediatos en cada mensaje fallido.

Según la especificación, un receptor **debe** adherirse a la política anunciada. Si no lo hacen, **deben** notificar al propietario del dominio del remitente en el informe agregado.

El concepto central de DMARC es la llamada alineación de identificadores. La alineación del identificador define cómo un mensaje puede pasar la verificación de DMARC. Los identificadores SPF y DKIM se alinean por separado, y un mensaje debe pasar **cualquiera** de ellos para pasar DMARC en general. Sin embargo, existe una opción de política de DMARC en la que el remitente puede solicitar que se genere un informe de fallos incluso si se supera una alineación, pero la otra falla. Podemos ver esto en el ejemplo anterior con la etiqueta "fo" configurada en "1".

Hay dos formas de que los mensajes se adhieran a la alineación de identificadores DKIM o SPF, estricta y relajada. La adhesión estricta significa que el FQDN del encabezado de debe coincidir completamente con el ID de dominio de firma ("d" tag) de la firma DKIM o FQDN del comando MAIL FROM SMTP para SPF. Relajado, por otra parte, permite que Header From FQDN sea un subdominio de los dos anteriores mencionados. Esto tiene importantes implicaciones al delegar el tráfico de correo electrónico a terceros, que se tratarán más adelante en el documento.

Consideraciones sobre la implementación de SPF

SPF para receptores

La verificación SPF es trivial para configurar en los dispositivos virtuales Cisco Email Security Appliance o Cloud Email Security. Para el resto de este documento, cualquier referencia a la ESA también incluirá CES.

La verificación SPF se configura en Políticas de flujo de correo; la forma más sencilla de ejecutarla globalmente es activarla en la sección Parámetros de política predeterminada de los receptores adecuados. Si está utilizando el mismo receptor para la recolección de correo entrante y saliente, asegúrese de que su política de flujo de correo "RELAYED" tenga la verificación SPF establecida en "Off".

Dado que SPF no permite la especificación de la acción de política a tomar, la verificación SPF (así como DKIM, como veremos más adelante) solamente verifica el mensaje e inserta un conjunto de encabezados para cada verificación SPF realizada:

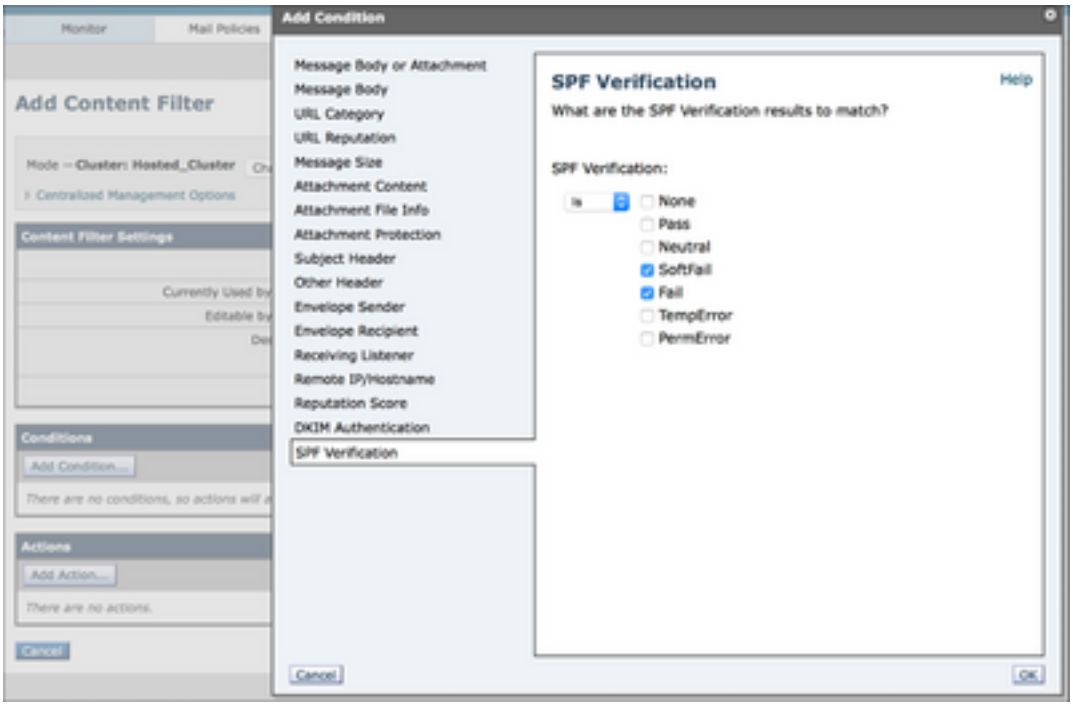
```
SPF recibido: Pass (mx1.hc4-93.c3s2.smtpi.com: dominio de

  united.5765@envfrm.rsys2.com designa 12.130.136.195 como

  allowed sender) identity=mailfrom;

  client-ip=12.130.136.195; receive=mx1.hc4-93.c3s2.smtpi.com;
```

```
  sobre-from="united.5765@envfrm.rsys2.com";

  x-sender="united.5765@envfrm.rsys2.com";

  x-conformance=sidf_compatible; x-record-type="v=spf1"

SPF recibido: Ninguno (mx1.hc4-93.c3s2.smtpi.com: no sender

  información de autenticidad disponible desde el dominio de

  postmaster@omp.news.united.com) identity=helo;

  client-ip=12.130.136.195; receive=mx1.hc4-93.c3s2.smtpi.com;

  sobre-from="united.5765@envfrm.rsys2.com";

  x-sender="postmaster@omp.news.united.com";

  x-conformance=sidf_compatible
```

Tenga en cuenta que para este mensaje, SPF verificó dos "identidades": "mailfrom" según lo dispuesto en la especificación, y "helo" según lo recomendado por la misma. El mensaje pasará formalmente el SPF, ya que sólo el primero es relevante para el cumplimiento de SPF, pero algunos receptores pueden sancionar a los remitentes que no incluyen registros SPF para sus identidades HELO también. Por lo tanto, es una buena práctica incluir los nombres de host de sus gateways de correo saliente en sus registros SPF.

Una vez que las políticas de flujo de correo verifican un mensaje, los administradores locales deben configurar una acción que se debe realizar. Esto se realiza utilizando la regla de filtro de mensajes SPF-status() [3], o creando un filtro de contenido entrante usando el mismo y aplicándolo a las políticas de correo entrante apropiadas.

Imagen 1: Condición de filtro de contenido de verificación SPF



Las acciones de filtrado recomendadas son descartar mensajes que fallan ("-all" en el registro SPF) y poner en cuarentena los mensajes que Softfail ("~all" en el registro SPF) en una cuarentena de políticas; sin embargo, esto puede variar según sus requisitos de seguridad. Algunos receptores solo etiquetan mensajes fallidos o no realizan ninguna acción visible, sino que los informan a los administradores.

Recientemente ha habido un aumento significativo en la popularidad de SPF, pero muchos dominios publican registros SPF incompletos o incorrectos. Para estar en el lado seguro, puede querer poner en cuarentena todos los mensajes que fallan en SPF, y monitorear la cuarentena durante un tiempo, para asegurarse de que no haya "falsos positivos".

Si Proporciona Servicios De Correo Electrónico Para Otros Dominios O Terceros

Si proporciona servicios de envío de correo electrónico o alojamiento para terceros, tendrán que agregar nombres de host y direcciones IP que utilice para enviar sus mensajes a sus propios registros SPF. La forma más sencilla de hacerlo es que el proveedor cree un registro SPF "general" y haga que los clientes utilicen el mecanismo "incluir" en sus registros SPF.

```
suncountry.com texto = "v=spf1 mx ip4:207.238.249.242 ip4:146.88.177.148
ip4:146.88.177.149 ip4:67.109 .66.68 ip4:198.179.134.238
ip4:107.20.247.57 ip4:207.87.182.66 ip4:199.66.248.0/22 incluir:cust-
spf.exacttarget.com ~all"
```

Como podemos ver, Sun Country tiene algunos de sus correos electrónicos bajo su propio control, pero su correo electrónico de marketing se subcontrata a un tercero. La ampliación del registro mencionado revela una lista de las direcciones IP actuales que utiliza su proveedor de servicios de correo de marketing:

```
cust-spf.exacttarget.com texto = " v=spf1 ip4:64.132.92.0/24
ip4:64.132.88.0/23 ip4:66.231.80.0/20
ip4:68.232.192.0/204:199.122.120.0/21
ip4:207.67.38.0/244:207.67.98.192/274:207.250.68.0/24 ip4:2099
.43.22.0/28 ip4:198.245.80.0/20 ip4:136.147.128.0/20
ip4:136.147.176.0/20 ip4:13.111.0.0/18 -all"
```

Esta flexibilidad permite a los proveedores de servicios de correo electrónico escalar sin tener que ponerse en contacto con cada cliente para modificar sus registros DNS.

Si Utiliza Servicios De Correo Electrónico De Terceros

De forma similar al párrafo anterior, si utiliza algún servicio de correo electrónico de terceros y desea establecer un flujo de correo totalmente verificado por SPF, debe incluir sus propios registros SPF en el suyo.

```
jetblue.com texto descriptivo "v=spf1 include:_spf.qualtrics.com ?all"
```

JetBlue utiliza el servicio de análisis Qualtrics y lo único que necesitan es incluir un registro SPF correcto de Qualtrics. Del mismo modo, la mayoría de los otros ESP proporcionan registros SPF que se incluirán en los registros de sus clientes.

Si su ESP o el marcador de correo electrónico no proporcionan registros SPF, tendrá que enumerar sus gateways de correo saliente directamente en el suyo. Sin embargo, es

responsabilidad suya mantener esos registros exactos, y si el proveedor agrega gateways adicionales o cambia direcciones IP o nombres de host, su flujo de correo puede estar en peligro.

El peligro adicional de terceros que no están preocupados por SPF proviene del uso compartido de recursos: Si un ESP utiliza la misma dirección IP para enviar correo electrónico de varios clientes, es técnicamente posible que un cliente genere un mensaje válido para SPF que pretenda ser otro cliente que entrega a través de la misma interfaz. Esta es la razón por la que, antes de establecer cualquier restricción SPF, debe investigar las políticas de seguridad de su MSP y el reconocimiento de la autenticación de correo electrónico. Si no tienen respuesta a sus preguntas, teniendo en cuenta que SPF es uno de los mecanismos básicos de confianza en Internet, se recomienda encarecidamente que reconsidere su elección de MSP. No se trata sólo de la seguridad: las mejores prácticas de SPF, DKIM, DMARC y otros remitentes [4] empleadas por los MSP son una garantía de la entrega. Si su MSP no los sigue o no los sigue correctamente, disminuirá su fiabilidad con los grandes sistemas receptores y posiblemente retrasará o incluso bloqueará sus mensajes.

(Sub)Dominios sin tráfico de correo electrónico

Actualmente, la mayoría de las organizaciones poseen varios dominios con fines de marketing, pero solo utilizan uno de forma activa para el tráfico de correo electrónico corporativo. Incluso si SPF se implementa correctamente en el dominio de producción, los agentes inadecuados pueden seguir utilizando otros dominios que no se utilizan activamente en un correo electrónico para simular la identidad de una organización. SPF puede evitar que esto ocurra a través de un registro SPF especial "deny all" (negar todo), para cualquiera de sus dominios (¡y subdominios!) que no generen tráfico de correo electrónico, publique "v=spf1 -all" en el DNS. Un excelente ejemplo es openspf.org - el sitio web del Consejo SPF.

Puesto que la delegación de SPF es válida sólo para un único dominio, también es fundamental publicar "denegar todos" los registros SPF de cualquier subdominio que esté utilizando y que pueda no generar un correo electrónico. Incluso si su dominio de producción tiene un registro SPF "regular", realice un esfuerzo adicional para agregar registros "denegar todos" a sus subdominios sin tráfico. Y, de nuevo, no olvide que recibir no equivale a enviar: Es muy posible que un dominio esté recibiendo correo electrónico, pero nunca será una fuente. Esto es muy cierto en el caso de los dominios de marketing a corto plazo (por ejemplo, eventos, promociones de tiempo limitado, lanzamientos de productos...), en los que los mensajes de correo electrónico entrantes en esos dominios se enviarían a su dominio de producción, y cualquier respuesta a dichos correos se entregaría desde el dominio de producción. Estos dominios a corto plazo tendrán un registro MX válido pero deberían tener un registro SPF que los identifique como **origen** de correo electrónico también.

Consideraciones sobre la implementación de DKIM

DKIM para receptores

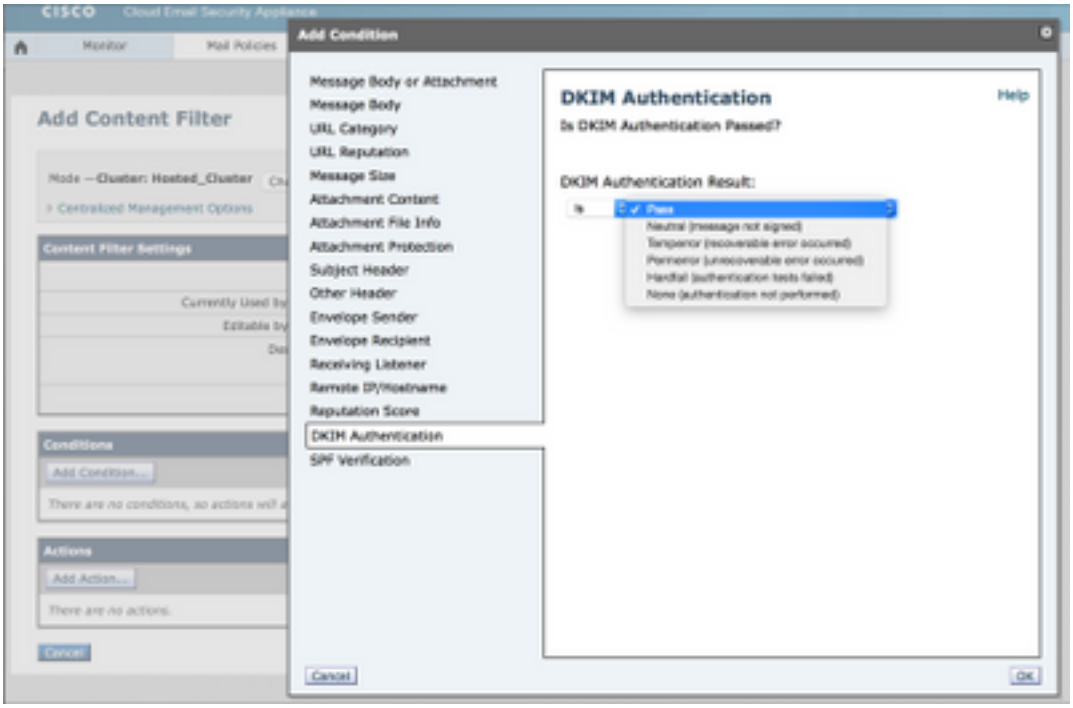
La configuración de la verificación DKIM en el ESA es similar a la verificación SPF. En los Parámetros de Política Predeterminados de las Políticas de Flujo de Correo, simplemente active la Verificación DKIM en "On". Una vez más, dado que DKIM no permite ninguna especificación de política, esto simplemente verificará la firma e insertará un encabezado "Authentication-Results" (Resultados de autenticación):

```
Resultados de autenticación: mx1.hc4-93.c3s2.smtpi.com; dkim=pass (firma
```

```
verificada) header.i=MileagePlus@news.united.com
```

Los filtros de contenido deben realizar cualquier acción basada en los resultados de la verificación DKIM:

Imagen 2: Condición de filtro de contenido de verificación DKIM



A diferencia de SPF, que es sencillo, DKIM manipula el texto real del mensaje, por lo que algunos parámetros pueden ser limitados. Opcionalmente, puede crear perfiles de verificación DKIM y asignar diferentes perfiles de verificación a diferentes políticas de flujo de correo. Le permiten limitar el tamaño de las firmas que aceptará, establecer acciones de falla de recuperación de claves y configurar la profundidad de la verificación DKIM.

Cuando un mensaje pasa varias puertas de enlace, se puede firmar varias veces y, por lo tanto, llevar varias firmas. Para que un mensaje pase la verificación DKIM, **cualquier** firma debe verificarse. De forma predeterminada, el ESA verificará hasta cinco firmas.

Debido a la apertura histórica de SMTP y correo electrónico y a la renuencia de Internet en general a adaptarse a cambios (positivos), todavía hay varias situaciones en las que las firmas DKIM pueden fallar legítimamente, como cuando los administradores de listas de correo retransmiten directamente pero modifican mensajes o cuando los mensajes se reenvían directamente en lugar de como adjuntos a nuevos mensajes. Esta es la razón por la que, en general, la mejor práctica para los mensajes que fallan en DKIM seguiría siendo ponerlos en cuarentena o etiquetarlos, en lugar de descartarlos.

Preparación para firmar con DKIM

Antes de activar la firma DKIM en la política de flujo de correo RELAYED, debe generar/importar las claves, crear perfiles de firma DKIM y publicar las claves públicas en el DNS.

Si firma un solo dominio, el proceso es sencillo. Genere el par de claves, cree su perfil de firma único en la sección Claves de dominio de Políticas de correo y haga clic en la opción "Generar" en "Registro de texto DNS" una vez que su perfil esté listo. Publique la clave tal como se generó

en el DNS. Finalmente, active la firma DKIM en su política de flujo de correo.

Se complica aún más si firma varios dominios distintos. En ese caso, tiene dos opciones:

1. Utilice un único perfil de firma para firmar para todos los dominios. Almacenará la clave pública (única) en la zona DNS del dominio "principal" y sus firmas DKIM harán referencia a esa clave. Esta técnica solía ser empleada por los ESP en el pasado, les permitía iniciar sesión a gran escala, sin tener que interactuar con el espacio DNS de cada cliente [5].
2. Cree un perfil de firma independiente para cada dominio para el que inicie sesión. Esto hace que la configuración inicial sea más compleja, pero proporciona una mayor flexibilidad en el futuro. Cree un par de claves para cada dominio, cree un perfil que especifique sólo un dominio (y sus subdominios) en la sección "Perfil de usuarios" y publique la clave pública relevante en la zona DNS de ese dominio en particular.

Aunque la opción 1 es más fácil de comenzar, recuerde que finalmente romperá el DMARC. Debido a que DMARC requiere que la ID de dominio de firma esté alineada con la de encabezado, la alineación del identificador con DKIM fallará. Puede salirse con la suya si configura su SPF correctamente y confiar en la alineación de identificadores SPF para pasar la verificación de DMARC.

Sin embargo, al implementar la opción 2 desde el principio, no tendrá que preocuparse por DMARC y es bastante fácil revocar o reconfigurar el servicio de firma para un solo dominio. Además, si proporciona **algunos** servicios de correo electrónico para un dominio de terceros, lo más probable es que deba obtener la clave para utilizarla (e importarla a su ESA). Esa clave será específica del dominio, por lo que tendrá que crear un perfil independiente.

Si Utiliza Servicios De Correo Electrónico De Terceros

En general, si utiliza firmas DKIM y descarga parte del procesamiento de correo electrónico (por ejemplo, correos electrónicos de marketing) a un tercero, no desea que utilicen las mismas claves que utiliza en producción. Esta es una de las principales razones de la existencia de Selectores en DKIM. En su lugar, debe generar un nuevo par de claves, publicar la parte pública en su zona DNS y entregar la clave secreta a la otra parte. Esto también le permitirá revocar rápidamente esa clave concreta en caso de problemas mientras mantiene su infraestructura DKIM de producción intacta.

Aunque no es necesario para DKIM (los mensajes para el mismo dominio se pueden firmar con varias claves diferentes), es una buena práctica proporcionar un subdominio independiente para cualquier correo electrónico que sea manejado por un tercero. Facilitará el seguimiento de los mensajes y permitirá una implementación mucho más limpia de DMARC más adelante. Como ejemplo, considere estos cinco encabezados DKIM-Signature de varios mensajes de Lufthansa:

```
Firma DKIM: v=1; a=rsa-sha1; c=relajado/relajado; s=lufthansa;
d=boletín.milesandmore.com;

Firma DKIM: v=1; a=rsa-sha1; c=relajado/relajado; s=lufthansa2;
d=boletín.lufthansa.com;

Firma DKIM: v=1; a=rsa-sha1; c=relajado/relajado; s=lufthansa3;
d=lh.lufthansa.com;

Firma DKIM: v=1; a=rsa-sha1; c=relajado/relajado; s=lufthansa4;
```

```
d=e.milesandmore.com

Firma DKIM: v=1; a=rsa-sha1; c=relajado/relajado; s=lufthansa5; d=fly-
lh.lufthansa.com;
```

Podemos ver que Lufthansa está usando cinco claves diferentes (selectores) divididas en cinco subdominios separados de dos dominios de producción primarios (lufthansa.com y milesandmore.com). Esto significa que cada uno de ellos puede controlarse de forma independiente y cada uno puede externalizarse a un proveedor de servicios de mensajería diferente.

Consideraciones sobre la implementación de DMARC

DMARC Para Receptores

La verificación de DMARC en el ESA se basa en el perfil, pero a diferencia de DKIM, el perfil predeterminado se debe editar para cumplir con la especificación. El comportamiento predeterminado del ESA es no descartar ningún mensaje a menos que el cliente lo indique explícitamente, por lo que el perfil de verificación de DMARC predeterminado tendrá todas las acciones configuradas en "Sin acción". Además, para activar la generación correcta de informes, tendrá que editar "Configuración global" de la sección DMARC de "Políticas de correo".

Una vez que se ha configurado un perfil, la verificación de DMARC, al igual que las otras dos, se establece en la sección Configuración de política predeterminada de Políticas de flujo de correo. Asegúrese de marcar la casilla para enviar informes de comentarios agregados; esta es posiblemente la función más importante de DMARC para el remitente. En el momento de escribir este artículo, ESA no admite la generación de informes de errores por mensaje ("ruf" de la política DMARC).

Como las acciones de políticas de DMARC son aconsejadas por el remitente, a diferencia de SPF o DKIM, no hay acciones específicas configurables fuera de la configuración del perfil. No es necesario crear ningún filtro de contenido.

La verificación de DMARC agregará campos adicionales al encabezado Authentication-Results:

```
Resultados de autenticación: mx1.hc4-93.c3s2.smtpi.com; dkim=pass (firma
verificada) header.i=MileagePlus@news.united.com; dmarc=pass (p=none
dis=none) d=news.united.com
```

En el ejemplo anterior, vemos que se verificó el DMARC en función de la alineación del identificador DKIM y el remitente solicitó la política de "ninguno". Esto indica que se encuentran actualmente en la fase de "supervisión" de la implementación de DMARC.

Si Proporciona Servicios De Correo Electrónico Para Otros Dominios O Terceros

La mayor preocupación de los ESP por el cumplimiento de DMARC es lograr una correcta alineación de los identificadores. Al planificar el DMARC, asegúrese de que el SPF está configurado correctamente, de que todos los demás dominios relevantes tienen sus gateways salientes en sus registros SPF y de que no envían mensajes que no se ajustarán correctamente, principalmente mediante el uso de diferentes dominios para la identidad MAIL FROM y Header From. Este error lo suelen hacer las aplicaciones que envían notificaciones o advertencias por

correo electrónico, ya que los autores de las aplicaciones en su mayoría no son conscientes de las consecuencias de la incoherencia de sus identidades de correo electrónico.

Como se ha descrito anteriormente, asegúrese de utilizar un perfil de firmas DKIM independiente para cada dominio y de que su perfil de firmas haga referencia correctamente al dominio para el que está firmando como se utiliza en el encabezado De. Si utiliza sus propios subdominios, **puede** firmar con una única clave, pero asegúrese de establecer su adhesión a DKIM para que se relaje en la política DMARC ("adkim="r").

En general, si proporciona servicios de correo electrónico a un mayor número de terceros sobre los que no tiene control directo, es recomendable escribir un documento de guía sobre cómo enviar un correo electrónico que sea más probable que se envíe. Dado que el correo electrónico de usuario a usuario se comporta bien en general, esto servirá principalmente como documento de política para los autores de aplicaciones en los ejemplos mencionados anteriormente.

Si Utiliza Servicios De Correo Electrónico De Terceros

Si utiliza terceros para entregar parte del tráfico de correo electrónico, la forma óptima es delegar un subdominio independiente (o un dominio completamente diferente) al proveedor de terceros. De esta manera, pueden administrar los registros SPF según sea necesario, tener una infraestructura de firmas DKIM independiente y no interferir con el tráfico de producción. A continuación, la política de DMARC para el correo electrónico subcontratado puede ser diferente a la de los internos. Como ya se ha mencionado, al considerar el correo electrónico enviado por un tercero, asegúrese siempre de que sus identificadores estén alineados, y su cumplimiento de DKIM y SPF se establece adecuadamente en su política DMARC.

(Sub)Dominios sin tráfico de correo electrónico

Otra mejora de DMARC con respecto a las tecnologías de autenticación de correo electrónico anteriores es cómo gestiona los subdominios. De forma predeterminada, la política DMARC de un dominio determinado se aplica a todos sus subdominios. Al recuperar los registros de políticas de DMARC, si no se encuentra ningún registro en el nivel de encabezado desde FQDN, los receptores están obligados a determinar el dominio organizativo [6] del remitente y a buscar un registro de política allí.

Sin embargo, la política de DMARC para un dominio de organización también puede especificar una política de subdominio independiente ("sp" de un registro de DMARC) que se aplicará a cualquier subdominio que no tenga una política de DMARC explícita publicada.

En la situación descrita anteriormente en el capítulo SPF, debería:

1. Publica un registro de DMARC explícito para cualquier subdominio que **sea** fuente legítima de correo electrónico.
2. Publicar una política de subdominio de "rechazar" en su registro de política de dominio organizativo para rechazar automáticamente cualquier correo electrónico que falsifique dominios que no envíen

Este tipo de estructuración de la autenticación de correo electrónico proporciona la mejor protección posible de su infraestructura y marca.

Problemas específicos de DMARC

Existen varios problemas potenciales con DMARC, todos los cuales provienen de la naturaleza y las deficiencias de otras tecnologías de autenticación a las que se basa. El problema es que DMARC sacó a la superficie estos problemas al presionar activamente una política para rechazar el correo electrónico y correlacionar todos los diferentes identificadores de remitente en un mensaje.

La mayoría de los problemas se producen con las listas de correo y el software de administración de listas de correo. Cuando un correo electrónico se envía a una lista de correo, se redistribuye a todos sus destinatarios. Sin embargo, el correo electrónico resultante, con una dirección de remitente del remitente original, será enviado por la infraestructura de alojamiento del gestor de la lista de correo, por lo que las comprobaciones SPF de encabezado de (la mayoría de los administradores de la lista de correo utilizan la dirección de lista como Sobre de (CORREO DE) y la dirección del remitente original como Encabezado de).

Dado que DMARC fallará para SPF, podemos confiar en DKIM, sin embargo, la mayoría de los gerentes de listas de correo también agregan pies de página a los mensajes, o etiquetan temas con el nombre de la lista, rompiendo así la verificación de la firma DKIM.

Los autores de DKIM sugieren varias soluciones al problema, todas las cuales se reducen a que los administradores de la lista de correo tienen que utilizar la dirección de la lista en todas las direcciones From, e indican la dirección original del remitente por otro medio.

Problemas similares surgen de los mensajes que se reenvían simplemente copiando el mensaje original sobre SMTP al nuevo destinatario. Sin embargo, la mayoría de los agentes de usuario de correo que se utilizan hoy formarán correctamente un nuevo mensaje e incluirán el mensaje reenviado en línea o como adjunto al nuevo mensaje. Los mensajes reenviados de esta manera pasarán por DMARC si el usuario de reenvío pasa (por supuesto, no se puede establecer la autenticidad del mensaje original).

Plan De Acción De Ejemplo Para Implementar La Autenticación De Correo Electrónico

Aunque las tecnologías en sí son sencillas, el camino para implementar una infraestructura completa de autenticación de correo electrónico puede ser largo y sinuoso. Para las organizaciones más pequeñas y las que tienen flujos de correo controlados, será bastante sencillo, mientras que para los entornos más grandes puede resultar un reto excepcional. No es raro que las grandes empresas contraten servicios de consultoría para gestionar el proyecto de implementación.

Paso 1: DKIM

DKIM es relativamente poco intrusivo ya que los mensajes no firmados no incurrirán en ningún rechazo. Antes de la aplicación efectiva, tenga en cuenta todos los puntos mencionados anteriormente. Póngase en contacto con cualquier tercero al que pueda delegar la firma, asegúrese de que sus terceros admiten la firma de DKIM y considere su estrategia de gestión de selector. Algunas organizaciones conservarían claves separadas (selectores) para las distintas dependencias orgánicas. Puede considerar la rotación periódica de las claves para mayor seguridad, pero asegúrese de no eliminar las antiguas hasta que se entreguen todos los mensajes en tránsito.

Se debe prestar especial atención a los tamaños principales. Aunque en general "más es mejor",

debe tener en cuenta que la creación de dos firmas digitales por mensaje (incluida la canonicalización, etc.) es una tarea muy costosa para la CPU y puede influir en el rendimiento de los gateways de correo saliente. Debido a la sobrecarga de cálculo, 2048 bits es el tamaño de clave práctica más grande que se puede utilizar, pero en la mayoría de las implementaciones, las claves de 1024 bits suponen un buen riesgo entre el rendimiento y la seguridad.

Para una implementación posterior exitosa de DMARC, debe:

1. identifique todos los dominios que envíe como, incluidos los subdominios
2. generar claves DKIM y crear perfiles de firma para cada dominio
3. proporcionar claves privadas relevantes a terceros
4. publicar todas las claves públicas en zonas DNS relevantes
5. verificar que los terceros están listos para comenzar la firma
6. active la firma de DKIM en la política de flujo de correo RELAYED en todos sus ESA
7. notificar a terceros el inicio de la firma

Paso 2: SPF

Implementar adecuadamente SPF probablemente sea la parte más larga y engorrosa de cualquier implementación de infraestructura de autenticación de correo electrónico. Debido a que el correo electrónico era muy sencillo de usar y gestionar, y estaba completamente abierto desde el punto de vista de la seguridad y el acceso, las organizaciones tradicionalmente no aplicaban políticas estrictas sobre quién y cómo puede utilizarlo. Como consecuencia de ello, la mayoría de las organizaciones actuales no disponen de una vista completa de las diferentes fuentes de correo electrónico, tanto desde dentro como desde fuera. El mayor problema de la implementación de SPF es descubrir quién está enviando correos electrónicos legítimamente en su nombre.

Aspectos a buscar:

1. objetivos obvios: servidores Exchange u otros servidores de trabajo en grupo o gateways de correo saliente
2. cualquier solución DLP u otros sistemas de procesamiento de correo electrónico que puedan generar notificaciones externas
3. Sistemas CRM que envían información e interactúan con los clientes
4. varias aplicaciones de terceros que pueden enviar correo electrónico
5. laboratorio, pruebas u otros servidores que puedan enviar correo electrónico
6. ordenadores y dispositivos personales configurados para enviar un correo electrónico externo directamente

La lista anterior no está completa, ya que las organizaciones tienen entornos diferentes, pero debe considerarse como una directriz general sobre qué buscar. Una vez que se hayan identificado (la mayoría de) los orígenes de correo electrónico, es posible que desee dar un paso atrás y, en lugar de autorizar cada fuente existente, limpiar la lista. Lo ideal es que todos los correos salientes se envíen a través de los gateways de correo saliente con algunas excepciones justificadas. Si tiene su propia solución de correo de marketing o la utiliza, debería utilizar una infraestructura independiente que los gateways de correo electrónico de producción. Si su red de entrega de correo es excepcionalmente complicada, puede proceder a documentar el estado actual en su SPF, pero tome tiempo para limpiar la situación en el futuro.

Si presta servicio a varios dominios en la misma infraestructura, es posible que desee crear un

único registro SPF universal y hacer referencia a él en dominios individuales mediante el mecanismo "include". Asegúrese de que los registros SPF no sean demasiado amplios; Por ejemplo, si sólo cinco equipos de una red /24 envían SMTP, agregue esas cinco direcciones IP individuales a su SPF, en lugar de a toda la red. Intente que sus registros sean lo más específicos posible para minimizar las posibilidades de que un correo electrónico malintencionado ponga en peligro su identidad.

Comience con una opción softfail para remitentes que no coincidan ("~all"). Sólo cámbielo a hardfail (-all) una vez que esté 100% seguro de haber identificado **todas** sus fuentes de correo electrónico, de lo contrario se arriesga a perder el correo electrónico de producción. Más adelante, después de implementar DMARC y ejecutarlo en modo monitor durante un tiempo, podrá identificar cualquier sistema que haya perdido y actualizar sus registros SPF para que se complete. Sólo entonces será seguro configurar su SPF en hardfail.

Paso 3: DMARC

Una vez que el DKIM y el SPF se hayan configurado de la forma más completa posible, es el momento de crear las políticas de DMARC. Tenga en cuenta las diferentes situaciones mencionadas en los capítulos anteriores y prepárese para implementar más de un registro DMARC si dispone de una infraestructura de correo electrónico compleja.

Cree alias de correo electrónico que recibirán informes o cree una aplicación Web que pueda ingerirlos. No hay direcciones de correo electrónico estrictamente definidas que se puedan utilizar para esto, pero ayuda si son descriptivas, por ejemplo rua@domain.com, dmarc.rua@domain.com, mailauth-rua@domain.com, etc. Asegúrese de que dispone de un proceso para que un operador supervise estas direcciones y modifique la configuración SPF, DKIM y DMARC adecuadamente, o avise al equipo de seguridad en caso de una campaña de simulación. Inicialmente, la carga de trabajo será sustancial a medida que se ajusten los registros para cubrir todo lo que se haya perdido durante la configuración de SPF y DKIM. Después de un tiempo, los informes probablemente solo indicarán intentos de simulación.

Inicialmente, configure su política DMARC en "none" y su opción forense para enviar informes por **cualquier** comprobación fallida ("fo=1"); esto detectará rápidamente cualquier error en su SPF y DKIM sin influir en el tráfico. Una vez que esté satisfecho con el contenido de los informes enviados, cambie la política a "cuarentena" o "rechazo", en función de su política de seguridad y sus preferencias. De nuevo, asegúrese de que los operadores analizan continuamente los informes DMARC recibidos para detectar posibles falsos positivos.

Implementar DMARC completa y correctamente no es una tarea pequeña o corta. Si bien algunos resultados (y la "implementación" formal de DMARC) pueden obtenerse mediante la publicación de un conjunto incompleto de registros y una política de "ninguno", redunda en el mejor interés tanto de la organización remitente como de Internet en su conjunto que todo el mundo lo implemente en la medida de sus capacidades.

En cuanto a los plazos, aquí hay un esbozo muy aproximado de los pasos individuales para un proyecto típico. Una vez más, dado que cada organización es diferente, dista mucho de ser precisa:

1. Planificación y preparación de DKIM	2-4 semanas
2. ejecución de la prueba DKIM	2 semanas
3. SPF - identificación legítima del remitente	2-4 semanas
4. Preparación de la política de DMARC	2 semanas
5. Prueba de registros SPF y DMARC	4-8 semanas

6. Ejecución de prueba SPF con error	2 semanas
7. Prueba de DMARC ejecutada con cuarentena/rechazo	4 semanas
8. Supervisión de informes de DMARC y adaptación de SPF/DKIM en consecuencia	continuo

Es probable que las organizaciones más pequeñas experimenten una duración más corta en la mayoría de los pasos, especialmente en los pasos 3 y 4. Independientemente de lo sencilla que sea su infraestructura de correo electrónico, asigne siempre tiempo suficiente durante las ejecuciones de prueba y supervise estrechamente los informes de comentarios en busca de cualquier cosa que haya perdido.

Las organizaciones más grandes podrían experimentar una duración aún mayor de los mismos pasos, con requisitos de prueba más estrictos. No es raro que las empresas con una infraestructura de correo electrónico compleja contraten ayuda externa, no sólo por el aspecto técnico de la implementación de la autenticación de correo electrónico, sino también para gestionar todo el proyecto y coordinar entre equipos y departamentos.

Referencias adicionales

- El sitio de referencia para SPF: http://www.openspf.org
- El Consejo DKIM: http://www.dkim.org
- Sitio web principal de DMARC, administrado por The Trusted Domain Project: http://www.dmarc.org
- dmarcian - un sitio de ayuda y recursos dirigido por Tim Draegen, uno de los autores de DMARC. No olvide visitar la sección "Herramientas": http://www.dmarcian.com
- Herramienta Online Trust Alliance Record Validator: https://otalliance.org/resources/spf-dmarc-record-validator
- DMARC Record Assistant: otra herramienta útil para ayudarle a crear sus registros DMARC: http://www.kitterman.com/dmarc/assistant.html
- Herramientas de prueba de registros SPF: http://www.kitterman.com/spf/validate.html
- "No sea un pesadizo: Perspectiva en las técnicas de autenticación de correo electrónico", una presentación de Cisco Live 2014 BRKSEC-3770: https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=76627

[1] La canonicalización está fuera del alcance de este documento. Consulte el material de la sección "Referencias adicionales" para obtener más información sobre la canonicalización DKIM.

[2] Los parámetros del registro DNS DKIM también están fuera del alcance de este documento.

[3] La creación de filtros de mensajes está fuera del alcance de este documento. Consulte AsyncOS para obtener ayuda sobre las guías de usuario de correo electrónico.

[4] El M3AAWG definió un excelente conjunto de mejores prácticas aplicadas y respetadas por la mayoría de la industria. Su documento de mejores prácticas comunes para remitentes está disponible en https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf

[5] Este comportamiento aprovecha el hecho de que, originalmente, DKIM no verifica el origen del mensaje como se indica en MAIL FROM o Header From en absoluto. Solo verifica que el parámetro Signing Domain ID ("d" de la firma DKIM y el parámetro "Domain Name" en su perfil de firma) esté alojando la clave pública del par utilizado para firmar el mensaje. La autenticidad del

remitente se implica al tener el encabezado "From" firmado. Asegúrese de enumerar todos y cada uno de los dominios (y subdominios) que haya iniciado sesión en la sección "Perfil de usuarios".

[6] Normalmente, un dominio de un nivel por debajo de TLD o prefijo ccTLD relevante (.ac.uk, .com.sg etc...)