Arquitectura DMARC - Alineación del identificador

Contenido

Introducción

Este documento describe los conceptos de la arquitectura Dominio-basada general de la autenticación del mensaje, de la información y de la conformidad (DMARC), junto con los requisitos de la alineación del Marco de políticas del remitente (SPF) y de los DomainKeys Identified Mail (DKIM) en relación con DMARC.

Terminología

Esta sección describe y proporciona a la definición a algunos de los términos dominantes usados dentro de este documento.

- **EHLO/HELO** - Los comandos que suministran la identidad de un cliente SMTP durante la inicialización de una sesión de SMTP según lo definido en el RFC 5321.
- **De la encabezado** - De: el campo especifica a los autores de un mensaje. Incluirá típicamente el nombre de la visualización (qué es mostrado a un usuario final por el cliente del correo), junto con una dirección de correo electrónico que contenga una local-parte y un Domain Name (por ejemplo, “Juan Pérez” < johndoe@example.com >) según lo definido en el RFC 5322.
- **CORREO DE** - Esto se deriva del comando MAIL al inicio de una sesión de SMTP y proporciona a la identificación del remitente según lo definido en el RFC5321. También se conoce extensamente como el remitente del sobre, el trayecto de retorno o el direccionamiento de la despedida.

DMARC - Alineación del identificador

DMARC ata qué DKIM y SPF autentica a lo que se enumera en de la encabezado. Esto es hecha por la *alineación*. La alineación requiere que la identidad del dominio autenticada por el SPF y el DKIM hagan juego el dominio en la dirección de correo electrónico visible al usuario final.

Comencemos con es un qué identificador y porqué son importantes en referencia a DMARC.

Identificadores

Los identificadores identifican un Domain Name que se autenticará.

Identificadores en referencia a DMARC:

- SPF:

  El SPF autentica el dominio del cual aparece en el CORREO o la porción EHLO/HELO de la conversación SMTP, o ambos. Éstos pueden ser diversos dominios, y no son típicamente visibles al usuario final.

- DKIM:

  El DKIM autentica el dominio de firma que se pone a una firma dentro de la etiqueta del *d=*.

Estos (SPF y DKIM) identificadores se autentican contra el Identificador del dominio derivado en de la encabezado. Del dominio de la encabezado se utiliza porque es el campo más común del agente de usuario del correo (M.U.A.) para el terminal original del mensaje y es el que está usado por los usuarios finales para identificar la fuente del mensaje (un remitente), que también hace de la encabezado una blanco primera para el abuso.

> Precaución: DMARC puede proteger el abuso solamente contra un válido contra la encabezado.

DMARC no puede actuar encendido:

- Encabezados malformadas, ausentes o relanzadas del RFC 5322
- encabezados No-obedientes, pues no serán validadas
- Cuando hay más de una identidad del dominio en la encabezado (*)

Por lo tanto, un proceso además de DMARC debe existir para identificar los mensajes con las encabezados malformadas no-obedientes y para ejecutar una manera de marcarlas y de hacer visibles como encabezados elegibles no--DMARC.

(*) DMARC necesita extraer una sola identidad del dominio de la encabezado. Si hay más de una dirección de correo electrónico en la encabezado que esta encabezado será saltada en la mayoría de las puestas en práctica DMARC. Procesando las encabezados con más de una identidad del dominio se exponen como hacia fuera-de-alcance en la especificación DMARC.

Cuando Cisco ESA puede detectar más de una identidad del dominio deja un mensaje apropiado en los registros del correo:

```
(Machine esa.lab.local) (SERVICE)> grep -i "verification skipped" mail_logs

Tue Oct 16 14:13:52 2018 Info: MID 2003 DMARC: Verification skipped (Sending domain could not be determined)
```

Alineación del identificador

La alineación del identificador define una relación entre el dominio autenticado por el SPF y/o el DKIM y de la encabezado. La alineación es un proceso que corresponde con que las necesidades de ser encontrado además después de la verificación acertada del SPF y/o del DKIM. El proceso de autenticación DMARC requiere por lo menos uno de los identificadores (identidad del dominio) usados por el SPF o el DKIM que se alinearán con la porción del dominio del direccionamiento de la encabezado.

DMARC introduce dos modos de la alineación:

- el modo **estricto** requiere un exacto - haga juego (alinee) entre los Domain Name
- el modo **relajado** permite el subdomain del mismo dominio

Se requiere la alineación del identificador porque un mensaje puede llevar una firma válida de cualquier dominio, incluyendo los dominios usados por una lista de correo o aún un mún actor. Por lo tanto, simplemente llevar una firma válida no es bastante para deducir la autenticidad del dominio del autor.

Alineación DKIM

El Identificador del dominio DKIM es obtenido revisando la etiqueta del *d=* en una firma DKIM, y se compara con del dominio de la encabezado para verificar con éxito una firma DKIM.

Como un ejemplo, el mensaje se puede firmar en nombre del dominio d=blog.cisco.com, que identifica el dominio blog.cisco.com *como firmante.* DMARC utiliza este dominio y lo compara con la parte del dominio de la encabezado (por ejemplo, noreply@cisco.com). La alineación entre estos identificadores fallará en el strictmode pero pasará usando el modo relajado.

Note: Un solo correo electrónico puede contener las firmas múltiples DKIM, y se considera ser un DMARC “paso” si cualquier firma DKIM se alinea y verifica.

Alineación SPF

El mecanismo SPF (spfv1) autentica los Identificadores del dominio entregados de:

- CORREO de la identidad (comando mail from)
- Identidad HELO/EHLO (comando HELO/EHLO)

El CORREO de los intentos de la identidad del dominio que se autenticarán por abandono. La identidad del dominio HELO es autenticada por DMARC solamente para los mensajes con un CORREO vacío de la identidad, como los mensajes de despedida.

Un ejemplo común de esto sería adonde un mensaje se envía con un diverso CORREO del direccionamiento (noreply@blog.cisco.com) comparado a cuál está en de la encabezado (noreply@cisco.com). El CORREO de la parte de noreply **@blog.cisco.com de la** identidad del dominio **alineará con del** domainof noreply @cisco.com de la encabezado en el relaxedmode pero no en el modo estricto.

Etiquetas del modo de la alineación

Los modos de la alineación DMARC se pueden definir en un expediente de la directiva DMARC usando las etiquetas del modo de la alineación del **adkim** y del **aspf**. Estas etiquetas indican qué modo se requiere para alineación del identificador DKIM o SPF.

Los modos se pueden fijar a relajado o a estricto, con ser relajado el valor por defecto si no hay etiqueta presente. Esto se puede fijar bajo etiqueta-valor como:

- **r: modo relajado**
- **s: modo estricto**

Referencia

- RFC5321 - Protocolo Simple Mail Transfer
- RFC5322 - Internet Message format (Formato del mensaje)
- RFC6376 - Firmas de los DomainKeys Identified Mail (DKIM)
- RFC7208 - Marco de políticas del remitente (SPF) para el uso que autoriza de los dominios en el correo electrónico

- RFC7489 - autenticación del mensaje Dominio-basada, información, y conformidad (DMARC)