Architecture DMARC - Cadrage d'identifiant

Contenu

Introduction

Ce document des concepts décrit de message architecture basée sur domaine générale d'authentification, d'enregistrement et de conformité (DMARC), avec Sender Policy Framework (SPF) et des conditions requises de cadrage de la messagerie identifiées par DomainKeys (DKIM) par rapport à DMARC.

Terminologie

Cette section décrit et fournit la définition à certains des termes principaux utilisés dans ce document.

- **EHLO/HELO** - Les commandes qui fournissent l'identité d'un client de SMTP pendant l'initialisation d'une session de SMTP comme défini dans RFC 5321.
- **De l'en-tête** - De : le champ spécifie les auteurs d'un message. Il inclura typiquement le nom d'affichage (ce qui est affiché à un utilisateur par le client mail), avec une adresse e-mail qui contient une gens du pays-partie et un nom de domaine (par exemple, « daine de John » < johndoe@example.com >) comme défini dans RFC 5322.
- **MESSAGERIE DE** - Ceci est dérivé de la commande de MESSAGERIE au début d'une session de SMTP et fournit l'identification d'expéditeur comme défini dans RFC5321. On le connaît également largement comme expéditeur d'enveloppe, chemin de retour ou adresse de rebond.

DMARC - Cadrage d'identifiant

DMARC attache quels DKIM et SPF authentifient à ce qu'est répertorié dans de l'en-tête. Ceci est fait par *cadrage*. Le cadrage exige que l'identité de domaine a authentifié par la correspondance SPF et DKIM le domaine dans l'adresse e-mail visible à l'utilisateur final.

Commençons par quel identifiant est et pourquoi ils sont importants en référence à DMARC.

Identifiants

Les identifiants identifient un nom de domaine à authentifier.

Identifiants en référence à DMARC :

- SPF :

  La SPF authentifie le domaine dont apparaît dans la MESSAGERIE ou la partie EHLO/HELO de la conversation de SMTP, ou chacun des deux. Ceux-ci peuvent être différents domaines, et elles ne sont typiquement pas visibles à l'utilisateur final.

- DKIM :

  DKIM authentifie le domaine de signature qui est apposé à une signature dans la balise de *d=*.

Ces (SPF et DKIM) identifiants sont authentifiés contre l'identifiant de domaine dérivé dans de l'en-tête. Du domaine d'en-tête est utilisé parce que c'est le champ le plus commun d'agent d'utilisateur de messagerie (messagerie) pour le créateur du message et est celui utilisé par des utilisateurs finaux pour identifier la source de message (un expéditeur), qui fait également à partir de l'en-tête un premier objectif pour l'abus.

> **Attention** : DMARC peut protéger l'abus seulement contre un valide contre l'en-tête.

DMARC ne peut pas traiter :

- En-têtes mal formées, absentes ou répétées RFC 5322
- en-têtes Non-conformes, car ils ne seront pas validés
- Quand il y a plus d'une identité de domaine dans l'en-tête (*)

Par conséquent, un processus en plus de DMARC devrait exister pour identifier des messages avec les en-têtes mal formées non-conformes et pour implémenter une manière de les marquer et de rendre visibles comme en-têtes éligibles de non-DMARC.

(*) DMARC doit extraire une identité simple de domaine de l'en-tête. S'il y a plus d'une adresse e-mail dans l'en-tête que cette en-tête sera ignorée dans la plupart des réalisations DMARC. Traitant des en-têtes avec plus d'une identité de domaine sont énoncés comme -de-portée dans la

spécification DMARC.

Quand Cisco ESA peut détecter plus d'une identité de domaine elle laisse un message approprié dans les logs de messagerie :

```
(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)
```

Cadrage d'identifiant

Le cadrage d'identifiant définit des relations entre le domaine authentifié par SPF et/ou DKIM et de l'en-tête. Le cadrage est un processus assorti qui les besoins d'être supplémentaire rencontré après vérification réussie de SPF et/ou de DKIM. La procédure d'authentification DMARC exige au moins un des identifiants (identité de domaine) utilisés par la SPF ou le DKIM à aligner avec la partie de domaine de l'adresse d'en-tête.

DMARC introduit deux modes de cadrage :

- le mode **strict** exige un précis - appariez (alignez) entre les noms de domaine
- le mode **décontracté** permet le sous-domaine du même domaine

Le cadrage d'identifiant est exigé parce qu'un message peut porter une signature valide de n'importe quel domaine, y compris des domaines utilisés par une liste de diffusion ou même un mauvais acteur. Par conséquent, porter simplement une signature valide n'est pas assez pour impliquer l'authenticité du domaine d'auteur.

Cadrage DKIM

L'identifiant de domaine DKIM est obtenu en passant en revue la balise de *d=* dans une signature DKIM, et il est comparé au du domaine d'en-tête pour vérifier avec succès une signature DKIM.

Comme exemple, le message peut être signé au nom du domaine d=blog.cisco.com, qui identifie le domaine blog.cisco.com *en tant que signataire.* DMARC utilise ce domaine et le compare à la pièce de domaine de l'en-tête (par exemple, noreply@cisco.com). Le cadrage entre ces identifiants échouera dans le strictmode mais passera utilisant le mode décontracté.

> **Note**: Un email simple peut contenir de plusieurs signatures DKIM, et il est considéré un DMARC « passage » si n'importe quelle signature DKIM est alignée et vérifie.

Cadrage SPF

Le mécanisme SPF (spfv1) authentifie des identifiants de domaine livrés de :

- MESSAGERIE de l'identité (MESSAGERIE de commande)
- Identité HELO/EHLO (commande HELO/EHLO)

La MESSAGERIE des essais d'identité de domaine à authentifier par défaut. L'identité de domaine d'HÉLICOPTÈRE est authentifiée par DMARC seulement pour des messages avec une MESSAGERIE vide d'identité, comme des avis de non-livraison.

Un exemple classique de ceci serait où un message est envoyé avec une MESSAGERIE différente de l'adresse (noreply@blog.cisco.com) comparée à ce qu'est dans de l'en-tête (noreply@cisco.com). La MESSAGERIE de la pièce d'identité de domaine noreply de **@blog.cisco.com alignera avec du** domainof d'en-tête noreply @cisco.com dans le relaxedmode mais pas en mode strict.

Balises de mode de cadrage

Des modes de cadrage DMARC peuvent être définis sur un enregistrement de stratégie DMARC utilisant des balises de mode de cadrage d'**adkim** et d'**aspf**. Ces balises indiquent quel mode est exigé cadrage pour DKIM ou SPF identifiant.

Des modes peuvent être placés à décontracté ou à strict, en présence d'être décontracté le par défaut si aucune balise n'est. Ceci peut être placé sous la balise-valeur en tant que :

- **r : mode décontracté**
- **s : mode strict**

Référence

- RFC5321 - Simple Mail Transfer Protocol
- RFC5322 - Format d'Internet message
- RFC6376 - DomainKeys a identifié des signatures de la messagerie (DKIM)
- RFC7208 - Sender Policy Framework (SPF) pour l'usage de autorisation des domaines dans l'email
- RFC7489 - authentification de message basée sur domaine, enregistrement, et conformité (DMARC)