DMARC アーキテクチャ-識別配置

目次

概要

この資料は送信側政策の枠組（SPF）および DomainKeys によって識別される Mail （DKIM）配置必要条件と共に DMARC に関連して一般のドメイン ベースのメッセージ認証、レポートおよび準拠（DMARC）アーキテクチャ概念、記述したものです。

用語

このセクションはいくつかのこの資料の内で使用されるキー タームに定義を掲載して説明します。

- **EHLO/HELO** - RFC 5321 で定義されたように SMTP セッションの初期化の間に SMTP クライアントのアイデンティティを供給するコマンド。
- **ヘッダから**-から: フィールドはメッセージの作成者を規定 します。 それは RFC 5322 で定義されたようにローカル一部およびドメイン名が（たとえば、「ジョン・ドウ」< johndoe@example.com >）含まれている eメールアドレスと共に一般的にディスプレイ名前が（表記されるか何がメール クライアントによってエンドユーザに）、含まれています。
- **MAIL FROM** -これは SMTP セッションのはじめに MAIL コマンドから得られ、RFC5321 で定義されたように送信側 識別を提供します。 それはまたエンベロープ 送信側、リターンパスまたはバウンス アドレスとして広く知られています。

DMARC - 識別配置

DMARC はヘッダからのにリストされているものへのかどんな DKIM および SPF 認証する結びます。 これは*配置*によってされます。 配置はドメイン識別が SPF および DKIM によって一致する目に見えるエンドユーザへの eメールアドレスのドメインを認証したことを必要とします。

なんと識別から開始しようある、そしてなぜそれらが DMARC について重要であるか。

識別

識別は認証されるべきドメイン名を識別します。

DMARC について識別:

- SPF:

  SPF は SMTP メッセージ交換の MAIL FROM または EHLO/HELO 部分に現われる、または両方とも認証しますドメイン。 これらは異なるドメインであるかもしれ一般的に エンドユーザに目に見えません。

- DKIM:

  DKIM は *d=* タグ内のシグ二チャに添付される署名ドメインを認証します。

これらの (SPF および DKIM) 識別はヘッダからで得られるドメイン識別に対して認証されます。 メッセージの発信元のための最もよくある Mail ユーザ エージェント (MUA) フィールドで、またヘッダから濫用のための主なターゲットを作るメッセージ (送信側) のもとを識別することをエンドユーザが使用する 1 時であるのでヘッダ ドメインから使用されます。

注意： DMARC はヘッダから有効なからだけ濫用を保護できます。

DMARC は動作できません:

- 不正 な、不在または繰り返された RFC 5322 ヘッダ
- 彼らが検証されないので、不適合なヘッダ
- ヘッダに複数のドメイン識別がある時 (*)

従って不適合で不正 な ヘッダが付いているメッセージを識別し、非DMARC 適格なヘッダとしてそれらをマークし、見えるようにする方法を設定するために、DMARC に加えるプロセスはあるはずです。

(*) DMARC はヘッダから単一 ドメイン識別を得る必要があります。 このヘッダよりヘッダのあれば複数の eメールアドレスはほとんどの DMARC 実装でスキップされます。 複数のドメイン識別のヘッダを処理して DMARC 仕様ののスコープとして示されます。

Cisco ESA は検出とき複数のドメイン識別メール ログで適切なメッセージを残します:

```
(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)
```

識別配置

識別配置は SPF によって認証されるドメインおよび/または DKIM 間の関係をおよびヘッダから定義します。 配置はその上に SPF や DKIM の正常な確認の後で会われる必要一致するプロセスです。 DMARC 認証プロセスはヘッダ アドレスからののドメイン部分と一直線に並ぶべき SPF か DKIM によって使用される識別（ドメイン識別）の少なくとも 1 つを必要とします。

DMARC は 2 つの配置モードをもたらします:

- **厳密な**モードはドメイン名間の完全に一致するものを（一直線に並べて下さい）必要とします
- **リラックスした**モードは同じドメインのサブドメインを可能にします

メッセージがメーリングリストまた更に悪いアクターが使用するドメインを含むあらゆるドメインからの有効なシグニチャに、耐えることができるので識別配置が必要となります。 従って、ただ有効なシグニチャに耐えることは作成者ドメインの信頼性を推論する十分ではないです。

DKIM 配置

DKIM ドメイン識別は DKIM シグニチャの *d=* タグの検討によって得られ、正常に DKIM シグニチャを確認することをヘッダ ドメインからのと比較します。

一例として、メッセージは*署名者として*ドメイン blog.cisco.com を識別するドメイン d=blog.cisco.com に代わって署名することができます。 DMARC はこのドメインを使用し、ヘッダからののドメイン部品と比較します（たとえば、noreply@cisco.com）。 これらの識別間の配置は strictmode に失敗しますが、リラックスしたモードを使用して渡ります。

> **注:** 単一 メールは複数の DKIM シグニチャが含まれている場合がありどの DKIM シグニチャでも一直線に並び、確認すれば DMARC 「パス」であることを考慮します。

SPF 配置

SPF （spfv1）メカニズムはから渡されるドメイン識別を認証します:

- MAIL FROM 識別（MAIL FROM コマンド）
- HELO/EHLO 識別（HELO/EHLO コマンド）

MAIL FROM ドメイン識別はデフォルトで認証されることを試みます。 ヘリコプター ドメイン識別はバウンス メッセージのような空 MAIL FROM 識別のメッセージのためのだけ DMARC によって、認証されます。

これの一般的な例は比較される別の MAIL FROM アドレス（noreply@blog.cisco.com）ヘッダ（noreply@cisco.com）からのにあるものとメッセージがと送信 されるところです。 noreply **@blog.cisco.com** の MAIL FROM ドメイン識別部品は relaxedmode のない厳密なモードのヘッダ domainof @cisco.com からの**と** noreply **一直線に並びます**。

配置モード タグ

DMARC 配置モードは **adkim** および **aspf** 配置モード タグを使用して DMARC ポリシー レコードで定義することができます。 これらのタグはどんなモードが DKIM または SPF 識別用に配置必要となるか示します。

モードはリラックスしたデフォルトであることとのリラックスしたか厳密にタグがない場合、設定 することができます。 これはタグ値の下でとして設定 することができます:

- **r: リラックスしたモード**
- **s： 厳密なモード**

参照

- RFC5321 - Simple Mail Transfer Protocol（SMTP）
- RFC5322 - インターネット メッセージ形式
- RFC6376 - DomainKeys は Mail（DKIM）シグニチャを識別しました
- RFC7208 - メールのドメインの承認使用のための送信側政策の枠組（SPF）
- RFC7489 - ドメイン ベースのメッセージ認証、レポートおよび準拠（DMARC）