Arquitetura DMARC - Alinhamento do identificador

Índice

Introdução

Este original descreve conceitos da arquitetura Domínio-baseada geral da autenticação de mensagem, do relatório e da conformidade (DMARC), junto com o quadro político do remetente (SPF) e exigências identificadas DomainKeys do alinhamento do correio (DKIM) com relação a DMARC.

Terminology

Esta seção descreve e fornece a definição a alguns dos termos chaves usados dentro deste original.

- **EHLO/HELO** - Os comandos que fornecem a identidade de um cliente de SMTP durante a iniciação de uma sessão de SMTP como definido no RFC 5321.
- **Do encabeçamento** - De: o campo especifica os autores de uma mensagem. Incluirá tipicamente o nome do indicador (o que é mostrado a um utilizador final pelo cliente do correio), junto com um endereço email que contenha uma local-parte e um Domain Name (por exemplo, “João da Silva” < johndoe@example.com >) como definido no RFC 5322.
- **CORREIO DE** - Isto é derivado do comando MAIL no início de uma sessão de SMTP e fornece a identificação do remetente como definido no RFC5321. É igualmente de conhecimento geral como o remetente do envelope, o caminho de retorno ou o endereço do salto.

DMARC - Alinhamento do identificador

DMARC amarra que DKIM e SPF autentica ao que é alistado no do encabeçamento. Isto é feito

pelo *alinhamento*. O alinhamento exige que a identidade do domínio autenticou pelo fósforo SPF e DKIM o domínio no endereço email visível ao utilizador final.

Deixe-nos começar com que identificador é e porque são importantes na referência a DMARC.

Identificadores

Os identificadores identificam um Domain Name a ser autenticado.

Identificadores na referência a DMARC:

- SPF:

  O SPF autentica o domínio de que aparece no CORREIO ou na parcela EHLO/HELO da conversação S TP, ou ambos. Estes podem ser domínios diferentes, e não são tipicamente visíveis ao utilizador final.

- DKIM:

  DKIM autentica o domínio de assinatura que é afixado a uma assinatura dentro da etiqueta do *d=*.

Estes (SPF e DKIM) identificadores são autenticados contra o identificador de domínio derivado no do encabeçamento. Do domínio do encabeçamento é usado porque é o campo o mais comum do agente de usuário do correio (M.U.A.) para o autor da mensagem e é esse usado por utilizadores finais para identificar a fonte da mensagem (um remetente), que igualmente faz do encabeçamento um alvo principal para o abuso.

Cuidado: DMARC pode proteger o abuso somente contra um válido do encabeçamento.

DMARC não pode operar-se sobre:

- Encabeçamentos deformados, ausentes ou repetidos do RFC 5322
- encabeçamentos NON-complacentes, porque não serão validados
- Quando houver mais de uma identidade do domínio no encabeçamento (*)

Consequentemente, um processo além do que DMARC deve existir para identificar mensagens com os encabeçamentos deformados NON-complacentes e para executar uma maneira de marcá-los e fazer visíveis como os encabeçamentos NON-DMARC elegíveis.

(*) DMARC precisa de extrair uma única identidade do domínio do encabeçamento. Se há mais de um endereço email no encabeçamento do que este encabeçamento estará saltado na maioria de aplicações DMARC. Processando encabeçamentos com mais de uma identidade do domínio são indicados como o para fora--espaço na especificação DMARC.

Quando Cisco ESA pode detectar mais de uma identidade do domínio deixa uma mensagem apropriada nos logs do correio:

```
(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)
```

Alinhamento do identificador

O alinhamento do identificador define um relacionamento entre o domínio autenticado pelo SPF e/ou DKIM e do encabeçamento. O alinhamento é um processo de harmonização que necessidades de ser encontrado adicionalmente após a verificação bem-sucedida do SPF e/ou do DKIM. O processo de autenticação DMARC exige pelo menos um dos identificadores (identidade do domínio) usados pelo SPF ou pelo DKIM a ser alinhados com a parcela do domínio de do endereço do encabeçamento.

DMARC introduz dois modos do alinhamento:

- o modo **restrito** exige um exato - combine (alinhe) entre Domain Name
- o modo **relaxado** permite o subdomínio do mesmo domínio

O alinhamento do identificador é exigido porque uma mensagem pode carregar uma assinatura válida de todo o domínio, incluindo os domínios usados por uma lista de endereços ou mesmo por um ator ruim. Consequentemente, meramente carregar uma assinatura válida não é bastante para pressupor a autenticidade do domínio do autor.

Alinhamento DKIM

O identificador de domínio DKIM é obtido revendo a etiqueta do *d= em uma* assinatura DKIM, e é comparado com do domínio do encabeçamento para verificar com sucesso uma assinatura DKIM.

Como um exemplo, a mensagem pode ser assinada em nome do domínio d=blog.cisco.com, que identifica o domínio blog.cisco.com *como um signatário.* DMARC usa este domínio e compara-o com o domínio parte de do encabeçamento (por exemplo, noreply@cisco.com). O alinhamento entre estes identificadores falhará no strictmode mas passará usando o modo relaxado.

Note: Um único email pode conter assinaturas múltiplas DKIM, e considera-se ser um DMARC “passagem” se qualquer assinatura DKIM é alinhada e verifica.

Alinhamento SPF

O mecanismo SPF (spfv1) autentica os identificadores de domínio entregados de:

- CORREIO da identidade (comando mail from)
- Identidade HELO/EHLO (comando HELO/EHLO)

O CORREIO das tentativas da identidade do domínio a ser autenticadas à revelia. A identidade do domínio HELO é autenticada por DMARC somente para mensagens com um CORREIO vazio da identidade, como mensagens de salto.

Um exemplo comum deste seria o lugar aonde uma mensagem é enviada com um CORREIO diferente do endereço (noreply@blog.cisco.com) comparado ao que está no do encabeçamento (noreply@cisco.com). O CORREIO da identidade parte de noreply **@blog.cisco.com do** domínio **alinhará com do** domainof noreply @cisco.com do encabeçamento no relaxedmode mas não no modo restrito.

Etiquetas do modo do alinhamento

Os modos do alinhamento DMARC podem ser definidos em um registro da política DMARC usando etiquetas do modo do alinhamento do **adkim** e do **aspf**. Estas etiquetas indicam que modo é exigido para alinhamento do identificador DKIM ou SPF.

Os modos podem ser ajustados a relaxado ou a restrito, com ser relaxado o padrão se nenhuma etiqueta esta presente. Isto pode ser ajustado sob o etiqueta-valor como:

- **r: modo relaxado**
- **s: modo restrito**

Referência

- RFC5321 - Protocolo Simples de Transferência de Correspondência (SMTP)
- RFC5322 - Formato de mensagem do Internet
- RFC6376 - DomainKeys identificou assinaturas do correio (DKIM)
- RFC7208 - Quadro político do remetente (SPF) para o uso de autorização dos domínios no email

- RFC7489 - autenticação de mensagem Domínio-baseada, relatório, e conformidade (DMARC)