RFC 8904 : DNS Whitelist (DNSWL) Email Authentication Method Extension

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 18 septembre 2020

Date de publication du RFC : Septembre 2020

https://www.bortzmeyer.org/8904.html

Le RFC 8601 [1] décrit un en-tête pour le courrier qui indique le résultat d'une tentative d'authentification. Cet en-tête `Authentication-Results:` permet plusieurs méthodes d'authentification, telles que SPF ou DKIM. Notre nouveau RFC 8904 ajoute une nouvelle méthode, `dnswl` (pour "*DNS White List*"), qui indique le résultat d'une lecture dans une liste blanche, ou liste d'autorisation via le DNS. Ainsi, si le client SMTP avait son adresse IP dans cette liste, un en-tête `Authentication-Results:` d'authentification positive sera ajouté.

Accéder via le DNS à des listes blanches (autorisation) ou des listes noires (rejet) de MTA est une pratique courante dans la gestion du courrier. Elle est décrite en détail dans le RFC 5782. Typiquement, le serveur SMTP qui voit une connexion entrante forme un nom de domaine à partir de l'adresse IP du client SMTP et fait une requête DNS pour ce nom et le type de données A (adresse IP). S'il obtient une réponse non-nulle, c'est que l'adresse IP figurait dans la liste (blanche ou noire). On peut aussi faire une requête de type TXT pour avoir du texte d'information. Ensuite, c'est au serveur SMTP de décider ce qu'il fait de l'information. La liste (noire ou blanche) lui donne une information, c'est ensuite sa responsabilité de décider s'il accepte ou rejette la connexion. La décision n'est pas forcément binaire, le serveur peut décider d'utiliser cette information comme entrée dans un algorithme de calcul de la confiance (« il est listé dans `bl.example`, 20 points en moins dans le calcul »).

Les plus connues des listes sont les listes noires (liste de clients SMTP mauvais) mais il existe aussi des listes blanches (liste de clients SMTP qu'on connait et à qui on fait confiance), et elles font l'objet de ce RFC. Il crée une nouvelle méthode pour l'en-tête `Authentication-Results:`, permettant ainsi d'enregistrer, dans un message, le fait qu'il ait été « authentifié » positivement via une liste blanche. On peut après se servir de cette « authentification » pour, par exemple, vérifier que le nom de domaine

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc8601.txt`

annoncé dans l'enregistrement TXT correspondant soit celui attendu (dans l'esprit de DMARC - RFC 7489 - ce qui est d'ailleurs très casse-gueule mais c'est une autre histoire).

Et le RFC fait un rappel utile : se servir d'une liste (noire ou blanche) gérée à l'extérieur, c'est sous-traiter. Cela peut être pratique mais cela peut aussi avoir des conséquences néfastes si la liste est mal gérée (comme le sont la plupart des listes noires, adeptes du « on tire d'abord et on négocie après »). Comme le dit le RFC, « vous épousez la politique du gérant de la liste ». Lisez aussi le RFC 6471, au sujet de la maintenance de ces listes.

La nouvelle méthode d'authentification (`dnswl`, section 2 de notre RFC) figure désormais dans le registre IANA des méthodes d'authentification <https://www.iana.org/assignments/email-auth/email-auth.xml#email-auth-methods>, spécifié dans le RFC 8601 (notamment section 2.7). Notre RFC 8904 décrit également les propriétés (RFC 8601, section 2.3 et RFC 7410) associées à cette authentification.

La méthode `dnswl` peut renvoyer `pass` (cf. le RFC 8601 pour ces valeurs renvoyées), qui indique que l'adresse IP du client est dans la liste blanche interrogée, `none` (client absent de la liste), ou bien une erreur (si la résolution DNS échoue). Contrairement à d'autres méthodes, il n'y a pas de résultat `fail`, ce qui est logique pour une liste blanche (qui liste les gentils et ne connait pas les méchants). Les principales propriétés possibles sont :

- `dns.zone` : le nom de domaine de la liste blanche,
- `policy.ip` : l'adresse IP renvoyée par la liste blanche, elle indique de manière codée les raisons pour lesquelles cette adresse est dans la liste,
- `policy.txt` : l'enregistrement TXT optionnel, peut indiquer le nom de domaine associé à ce client SMTP,
- `dns.sec` : indique si la requête DNS a été validée avec DNSSEC (`yes` si c'est le cas, `no` si la zone n'est pas signée, `na` si le résolveur <https://www.bortzmeyer.org/resolveur-dns.html> ne sait pas valider).

Le type `dns` pour les propriétés est une nouveauté de ce RFC, désormais enregistrée à l'IANA <https://www.iana.org/assignments/email-auth/email-auth.xml#property-types>.

La section 3 de notre RFC décrit l'enregistrement de type TXT qui donne des explications sur la raison pour laquelle l'adresse IP est dans la liste blanche (cf. RFC 5782, sections 2.1 et 2.2). Par exemple, il permet d'indiquer le domaine concerné (ADMD, "*ADministrative Management Domain*", cf. RFC 8601 pour ce concept).

Tiré de l'annexe A du RFC, voici un exemple d'un message qui a reçu un `Authentication-Results:`, qui contient les quatre propriétés indiquées plus haut :

```
Authentication-Results: mta.example.org;
     dnswl=pass dns.zone=list.dnswl.example dns.sec=na
     policy.ip=127.0.10.1
     policy.txt="fwd.example https://dnswl.example/?d=fwd.example"
```

Il se lit ainsi : le MTA `mta.example.org` estime son client authentifié par la méthode `dnswl` ("*DNS White List*") de ce RFC. La liste blanche a renvoyé la valeur `127.0.10.1` (sa signification exacte dépend de la liste blanche) et le TXT associé disait que le client SMTP appartenait au domaine `fwd.example`.

Dans l'exemple plus détaillé du RFC, le message avait été retransmis d'une manière qui cassait SPF et n'aurait donc pas été accepté sans la liste blanche, qui certifie que `fwd.example` est un retransmetteur connu et légitime.

Enfin, la section 5 du RFC traite de sécurité. Notamment, elle insiste sur le fait que le DNS n'est pas, par défaut, protégé contre diverses manipulations et qu'il est donc recommandé d'utiliser DNSSEC (ce que ne fait pas la liste blanche d'exemple citée plus loin).

Voyons maintenant des exemples avec une liste blanche réelle, . Prenons le serveur de messagerie de l'AFNIC, `2001:67c:2218:2::4:12`. On inverse l'adresse (par exemple, avec `ipv6calc -a 2001:67c:2218:2::4:12`) et on fait une requête sous `list.dnswl.org` :

```
% dig A 2.1.0.0.4.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0.8.1.2.2.c.7.6.0.1.0.0.2.list.dnswl.org
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1634
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 8, ADDITIONAL: 11
...
;; ANSWER SECTION:
2.1.0.0.4.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0.8.1.2.2.c.7.6.0.1.0.0.2.list.dnswl.org. 7588 IN A 127.0.9.1
...
;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Jul 04 09:16:37 CEST 2020
;; MSG SIZE  rcvd: 555
```

Que veut dire la valeur retournée, `127.0.9.1` ? On consulte la documentation de la liste <`https://www.dnswl.org/?page_id=15`> et on voit que 9 veut dire "*Media and Tech companies*" (ce qui est exact) et 1 "*low trustworthiness*". Il s'agit de la confiance dans le classement, pas dans le serveur. Pour le même serveur, la confiance est plus grande en IPv4 (3 au lieu de 1) :

```
% dig A 12.4.134.192.list.dnswl.org
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 266
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
12.4.134.192.list.dnswl.org. 10788 IN A 127.0.9.3
...
;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Jun 20 12:31:57 CEST 2020
;; MSG SIZE  rcvd: 72
```

Et les enregistrements TXT ? Ici, il valent :

```
% dig TXT 2.1.0.0.4.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0.8.1.2.2.c.7.6.0.1.0.0.2.list.dnswl.org
...
;; ANSWER SECTION:
2.1.0.0.4.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0.8.1.2.2.c.7.6.0.1.0.0.2.list.dnswl.org. 8427 IN TXT "nic.fr https://dnsw
```

En visant l'URL indiquée <https://dnswl.org/s/?s=8580>, on peut avoir tous les détails que la liste blanche connait de ce serveur. (Je n'ai pas investigué en détail mais j'ai l'impression que certains serveurs faisant autorité pour le domaine dnswl.org renvoient des NXDOMAIN à tort, par exemple sur les ENT - "*Empty Non-Terminals*" - ce qui pose problème si votre résolveur utilise une "*QNAME minimisation*" - RFC 9156 - stricte.)

Pour utiliser cette liste blanche depuis votre MTA favori, vous pouvez regarder la documentation de dnswl.org <https://www.dnswl.org/?page_id=15>. par exemple, pour Courier, ce sera :

```
-allow=list.dnswl.org
```

(Tous les détails dans la documentation de Courier <https://www.courier-mta.org/couriertcpd.html>). Pour Postfix, voyez la section dédiée dans la documentation de dnswl.org <https://www.dnswl.org/?page_id=15#postfix>. SpamAssassin, quant à lui, utilise dnswl.org par défaut.