Configuration des entrées SPF, DMARC et DKIM sur OVH offre MX PLAN

SPF indique les serveurs et domaines autorisés à envoyer des e-mails au nom de votre organisation.

DKIM est un système d'authentification des courriers électroniques qui vous aide à vérifier la légitimité de vos sources d'envoi et à vous assurer que le contenu de votre courrier électronique est resté inchangé tout au long du processus de livraison. DKIM ajoute une signature numérique à chaque message sortant pour permettre aux serveurs de réception de vérifier que le message provient bien de votre organisation.

DMARC permet d'indiquer aux serveurs de réception l'action à effectuer lorsque des messages sortants de votre organisation ne passent pas les contrôles SPF ou DKIM.

Configuration de SPF

- Sur l'interface d'OVH de gestion de la zone DNS du domaine, éditer l'enregistrement SPF ou en ajouter un.
- Indiquer l'IPv4 et l'IPv6 du serveur hébergent le domaine et le domaine mx.ovh.com d'OVH.
- Ex. d'enregistrement SPF : "v=spf1 a mx ip4:141.94.211.206 ip6:2001:41d0:304:400::a3e include:mx.ovh.com ~all"

Configuration de DMARC

- Sur l'interface OVH, au même endroit que l'enregistrement SPF (gestion de la zone DNS du domaine), cliquer sur le bouton "Ajouter une entrée" et choisir "DMARC"
- Compléter le formulaire ainsi :
    - Sous-domaine : _dmarc
    - TTL : par défaut
    - Version : DMARC1
    - Régle pour le domaine :
        - Lors de la première installation laisser : none
        - Une fois que vous avez vérifier que tout fonctionne depuis un certain temps basculer à : quarantine
        - Lorsque vous êtes certains que tout est OK passer à : reject
    - Pourcentage des messages filtrés : *laisser vide*
    - URI de création de rapports globaux : mailto:adminsys@<domaine-sinp>
    - Règle pour les sous-domaines : *laisser vide*
    - Mode d'alignement pour SPF : *ne rien cocher*

Configuration de DKIM

- Ressource :

https://help.ovhcloud.com/csm/fr-dns-zone-dkim?id=kb_article_view&sysparm_article=KB0058101

- Se rendre sur : https://api.ovh.com/console/
- Se connecter en cliquant sur le bouton "Authenticate" en haut à droite de la page
- Sur la gauche de la page, juste à côté du sélecteur de version d'API `v1`, taper `/email/domain/`
  - Filtrer la liste de web services en tapant `dkim` dans la zone de filtre juste au dessous, puis valider avec `Enter`
- **Vérifier l'activation de DKIM sur votre domaine** :
  - Sélectionner à l'aide la souris `GET /email/domain/{domain}/dkim`
  - Dans la section à droite `PATH PARAMETERS` et la zone de saisie `domain` indiquer le nom de domaine utilisé pour envoyer les emails.
    - Ex. adminsys@**silene.eu** ⇒ domain = silene.eu
  - Juste au dessous repérer le bouton TRY et cliquer dessus
  - Si DKIM est actif, le champ `status` de la réponse devrait avoir pour valeur `enabled`. Ex. de réponse :


```
{
  "activeSelector": "ovhmo3487488-selector1",
  "selectors": [
    {
      "cname": "ovhmo3487488-selector1._domainkey.silene.eu CNAME
ovhmo3487488-selector1._domainkey.3120053.ck.dkim.mail.ovh.net.",
      "selectorName": "ovhmo3487488-selector1",
      "status": "set"
    },
    {
      "cname": "ovhmo3487488-selector2._domainkey.silene.eu CNAME
ovhmo3487488-selector2._domainkey.3120052.ck.dkim.mail.ovh.net.",
      "status": "set",
      "selectorName": "ovhmo3487488-selector2"
    }
  ],
  "autoconfig": true,
  "status": "enabled"
}
```


    - Le champ `activeSelector` indique le nom du sélecteur DKIM actuellement utilisé par votre domaine.
    - Si le statut vaut `disabled`, il faut activer DKIM
- **Activer DKIM** :
  - L'activation indiqué ici est faite via l'API et ne fonctionne que si les emails sont envoyés via le serveur SMTP d'OVH. Mais il également possible de saisir manuellement une entée dans la Zone DNS du domaine en récupérant le sélecteur DKIM généré par OVH via l'API OVH. Voir la doc OVH indiquée en ressource ci-dessus. Cela permet ainsi d'ajouter plusieurs selecteurs DKIM a l'entrée DKIM de la zone DNS du domaine SINP utilisé pour l'envoi les emails.
  - Sélectionner à l'aide la souris `PUT /email/domain/{domain}/dkim/enable`
  - Dans la section à droite `PATH PARAMETERS` et la zone de saisie `domain` indiquer le nom de domaine utilisé pour envoyer les emails.
    - Ex. adminsys@**silene.eu** ⇒ domain = silene.eu
  - Juste au dessous repérer le bouton TRY et cliquer dessus

- Si tout va bien vous devriez obtenir une réponse du type :


```
{
 "domain": "mydomain.ovh",
 "id": 123455789,
 "function": "domain/enableDKIM",
 "status": "todo"
}
```


- **Tester le bon fonctionnement de DKIM** :
  - Envoyer un email via le serveur SMTP d'OVH vers une adresse de destination vérifiant DKIM
  - Dans la boite de réception en affichant l'original de l'email et ses entêtes vous devriez trouver dans les entêtes une entrée `Authentication-Results` :

```
Authentication-Results: mx.google.com;
       dkim=pass header.i=@silene.eu header.s=ovhmo3487488-
selector1 header.b=tKG01e8U;
       spf=pass (google.com: domain of mailer@silene.eu designates
178.33.251.173 as permitted sender)
smtp.mailfrom=mailer@silene.eu;
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=silene.eu
```

    - Si tout est ok, il y aura la valeur : **`dkim=pass`**

From:
https://wiki-sinp.cbn-alpin.fr/ - **CBNA SINP**

Permanent link:
https://wiki-sinp.cbn-alpin.fr/serveurs/installation/config-spf-dmarc-dkim

Last update: **2024/10/23 09:28**