Comment contourner le contrôle DMARC sur l'appliance de sécurité de la messagerie

Contenu

Introduction

Ce document décrit comment contourner la vérification DMARC (Domain-based Message Authentication, Reporting and Conformance) sur le dispositif de sécurité de la messagerie électronique (ESA). Référez-vous à Introduction sur l'authentification par e-mail.

Vérifier DMARC

DMARC est une spécification technique créée pour réduire le risque d'abus par e-mail. DMARC normalise la façon dont les destinataires de courriels effectuent l'authentification des courriels à l'aide des mécanismes Sender Policy Framework (SPF) et DomainKeys Identified Mail (DKIM). Pour réussir la vérification DMARC, un e-mail doit passer au moins un de ces mécanismes d'authentification et les identificateurs d'authentification doivent être conformes à la RFC 5322.

La solution matérielle-logicielle vous permet de :

- Vérifiez les e-mails entrants à l'aide de DMARC.
- Définissez les profils à substituer (accepter, mettre en quarantaine ou rejeter) aux stratégies des propriétaires de domaine.
- Envoyer des rapports de rétroaction aux propriétaires de domaines, ce qui contribue à renforcer leurs déploiements d'authentification.
- Envoyer des rapports d'erreurs de remise aux propriétaires de domaine si la taille du rapport global DMARC dépasse 10 Mo ou la taille spécifiée dans la balise RUA (Agrégations Report) de l'enregistrement DMARC.

AsyncOS peut gérer les e-mails conformes à la spécification DMARC telle qu'elle a été soumise à l'IETF (Internet Engineering Task Force) le 31 mars 2013. Pour plus d'informations, consultez http://tools.ietf.org/html/draft-kucherawy-dmarc-base-02.

> **Note**: L'appliance n'effectuera pas de vérification DMARC des messages provenant de domaines avec des enregistrements DMARC mal formés. Cependant, la solution matérielle-logicielle peut recevoir et traiter de tels messages.

Configurer le contournement DMARC

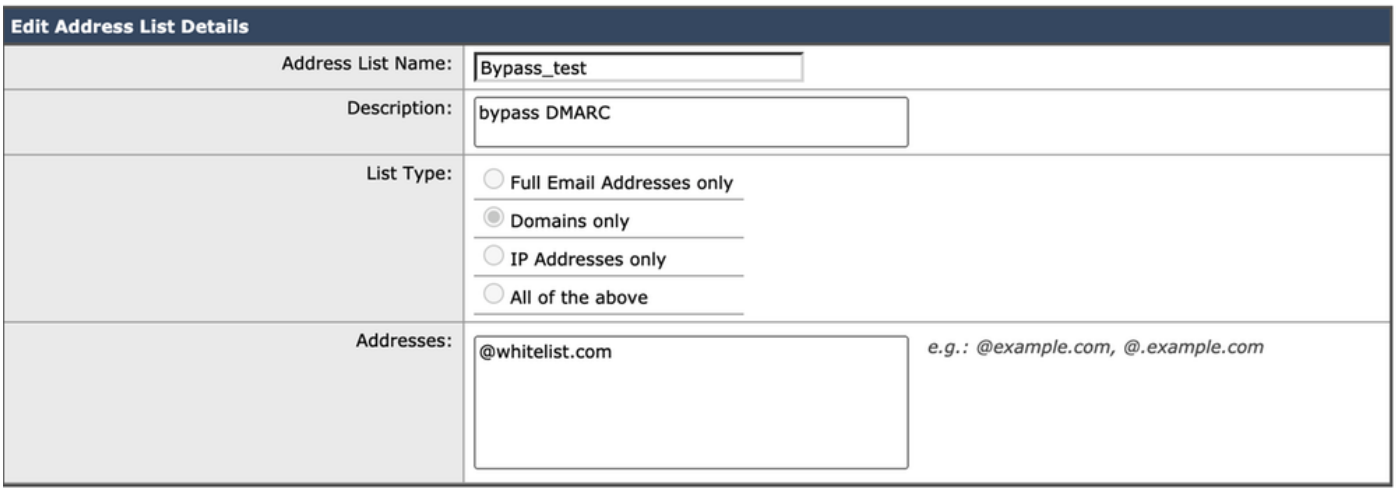
Si, en tant qu'administrateur, vous devez ignorer la vérification DMARC des messages provenant d'expéditeurs spécifiques, vous devrez suivre quelques étapes pour réussir le contournement. Vous trouverez ici un aperçu des étapes à suivre :

> **Note**: Les listes d'adresses créées avec l'utilisation d'adresses e-mail complètes ou de domaines peuvent uniquement être utilisées pour contourner la vérification DMARC. Vous pouvez utiliser une **liste d'adresses** avec l'option **Tous les éléments ci-dessus**. Cependant, les entrées avec uniquement une adresse e-mail complète/domaine ou une adresse de domaine partielle fonctionneront pour une exception. Vous devrez utiliser le **domaine/adresse e-mail complète** mentionné dans l'en-tête **De.**

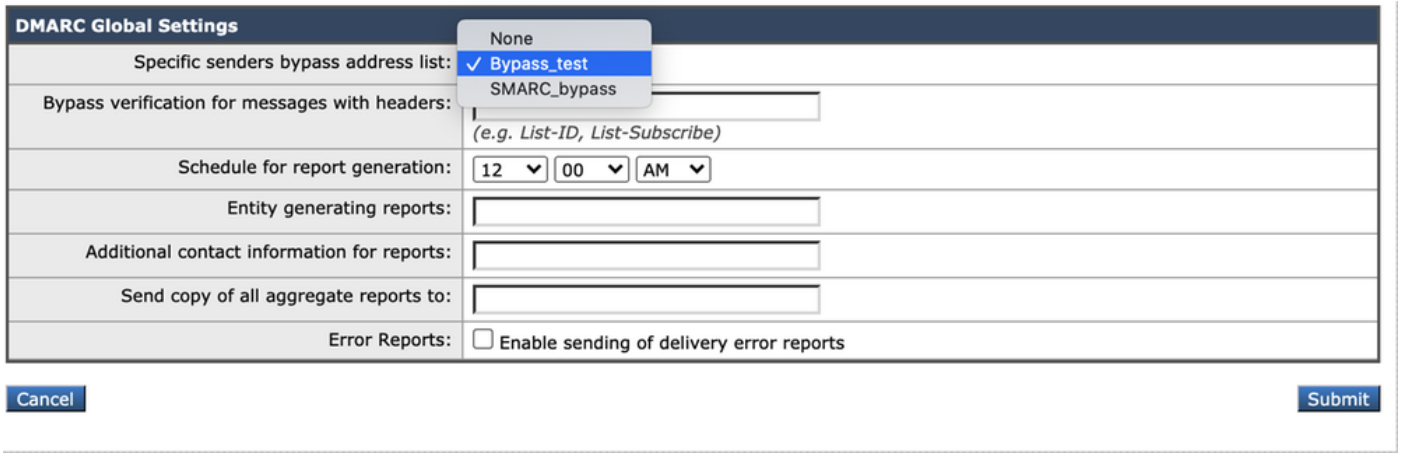
1. Assurez-vous que **la vérification DMARC** est activée pour la stratégie de flux de courrier associée.
2. Accédez à **Politiques de messagerie > Liste d'adresses**.
3. Cliquez sur **Ajouter une liste d'adresses**.
4. Créez une **liste d'adresses** en renseignant les détails.
5. Cliquez sur **Soumettre**.
6. Une fois la **liste d'adresses** créée, vous devez appeler la liste à la **liste d'adresses de contournement des expéditeurs DMARC spécifiques**.

Voici un exemple de configuration de contournement et de consignation :

La liste d'adresses est créée avec comme exemple "**Domains uniquement**" et est ajoutée dans les détails de l'en-tête **De.**



Une fois votre liste d'adresses créée avec toutes les entrées souhaitées, vous devrez appeler la **liste d'adresses** sous votre **liste d'adresses de contournement des expéditeurs spécifiques DMARC**. Vous devez naviguer jusqu'à **Politiques de messagerie > DMARC > Modifier les paramètres globaux** et appeler votre nouvelle **liste d'adresses** en cliquant sur la liste déroulante, comme indiqué ici :



Différence dans Mail_Logs

Une représentation de mail_logs est présentée ici, ce qui vous aidera à comprendre la différence entre la journalisation, quand le DMARC d'un domaine est validé et quand il est configuré pour sauter.

Journaux de messagerie lorsque DMARC est coché :

```
Sat Mar 20 21:14:22 2021 Info: ICID 57 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS rfc1918
country not applicable

Sat Mar 20 21:14:22 2021 Info: Start MID 76571 ICID 57

Sat Mar 20 21:14:22 2021 Info: MID 76571 ICID 57 From:

Sat Mar 20 21:14:22 2021 Info: MID 76571 ICID 57 RID 0 To:

Sat Mar 20 21:14:23 2021 Info: MID 76571 DMARC: Verification skipped (No record found for the
sending domain)

Sat Mar 20 21:14:23 2021 Info: MID 76571 DMARC:

Sat Mar 20 21:14:23 2021 Info: MID 76571 Message-ID '<613a1e1b-998a-6375-8887-
ab2c6d430256@whitelist.com>'

Sat Mar 20 21:14:23 2021 Info: MID 76571 Subject 'Test 4'
```

> **Note**: Il n'y a pas d'enregistrement publié pour le domaine @whitelist.com, c'est la raison pour laquelle nous voyons « Aucun enregistrement trouvé pour le domaine émetteur ».

Journaux de messagerie pour le contrôle DMARC de contournement

```
Sat Mar 20 21:15:36 2021 Info: ICID 58 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS rfc1918
country not applicable

Sat Mar 20 21:15:37 2021 Info: Start MID 76572 ICID 58

Sat Mar 20 21:15:37 2021 Info: MID 76572 ICID 58 From:
```

```
Sat Mar 20 21:15:37 2021 Info: MID 76572 ICID 58 RID 0 To:

Sat Mar 20 21:15:37 2021 Info: MID 76572 DMARC: Verification skipped (Local bypass
configuration)

Sat Mar 20 21:15:37 2021 Info: MID 76572 Message-ID '<2ba742a2-f8ba-9ff0-7dc9-
362421f5177e@whitelist.com>'

Sat Mar 20 21:15:37 2021 Info: MID 76572 Subject 'Test Bypass DMARC'
```

Informations connexes

- Présentation du workflow DMARC
- Comment vérifier les messages entrants à l'aide de DMARC
- Filtrer pour gérer les messages qui ont ignoré la vérification DMARC
- Support et documentation techniques - Cisco Systems