Guide de pratique recommandée pour des contrôles de vérification et de destination de rebond

Contenu

Introduction

La livraison à fort débit incontrôlée d'email peut accabler les domaines réceptifs. AsyncOS te donne le plein contrôle de la livraison de message en définissant le nombre de connexions que votre service de sécurité du courrier électronique s'ouvrira ou nombre de messages qui enverront à chaque domaine de destination.

Dans ce document, nous couvrirons :

1. Installation de la vérification de rebond pour protéger votre organisation contre des attaques de rebond
2. Utilisant le Tableau de contrôle de destination pour pratiquer de bonnes stratégies voisines
3. Déployer l'authentification basée sur dn de SMTP d'Entities (DANOIS) Désignée pour fournir la livraison sécurisée des messages

Vérification de rebond

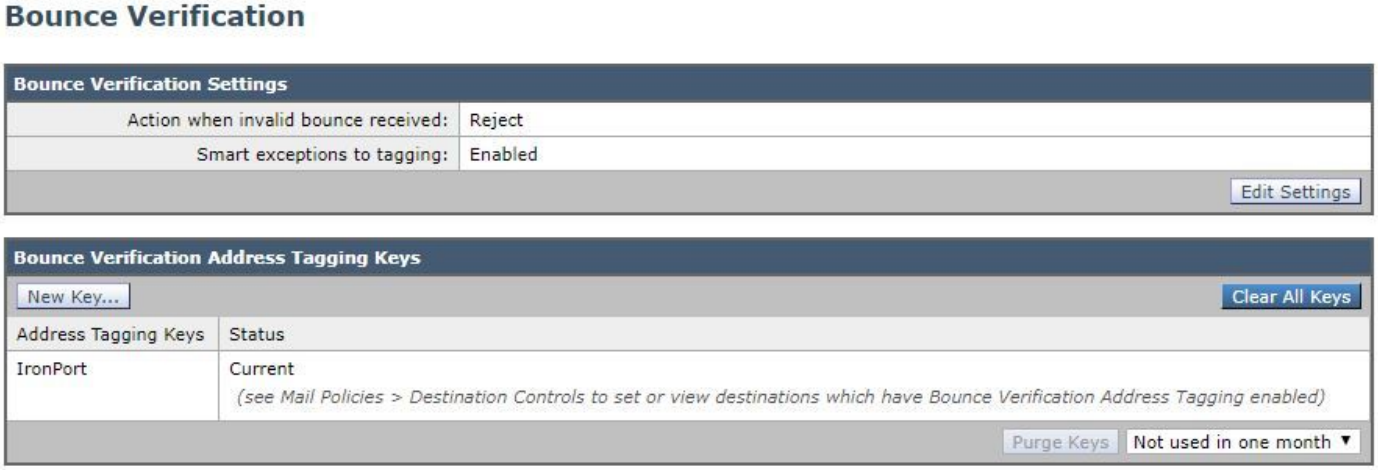
L'activation de la vérification de rebond est une manière très bonne de combattre des attaques de rétrodiffusion/rebond. Le concept derrière la vérification de rebond est simple. D'abord, marquez vers le haut des messages partant de votre ESA. Recherchez ce markup sur tous les avis de non-livraison, si le markup est présent, il signifie que c'est un rebond d'un message qui a provenu de votre environnement. Si le markup manque, le rebond est frauduleux et peut être rejeté ou abandonné.

Par exemple, MESSAGERIE DE : joe@example.com devient MESSAGERIE DE : prvs=joe=123ABCDEFG@example.com. … La chaîne 123 dans l'exemple est la balise de vérification de rebond qui est ajoutée à l'expéditeur d'enveloppe pendant qu'il est envoyé par votre appliance ESA. Si le message rebondit, l'adresse réceptive d'enveloppe dans le message rebondi inclura la balise de vérification de rebond, qui fait l'ESA savoir que c'est un message rebondi légitime.

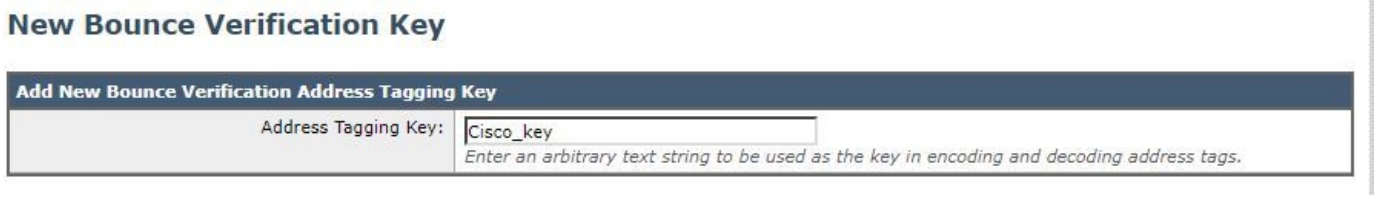
Vous pouvez activer ou désactiver la vérification de rebond étiquetant au niveau système comme par défaut. Vous pouvez également activer ou désactiver la vérification de rebond étiquetant pour les domaines spécifiques. Dans la plupart des déploiements, il est activé par défaut pour tous les domaines.

Configuration ESA

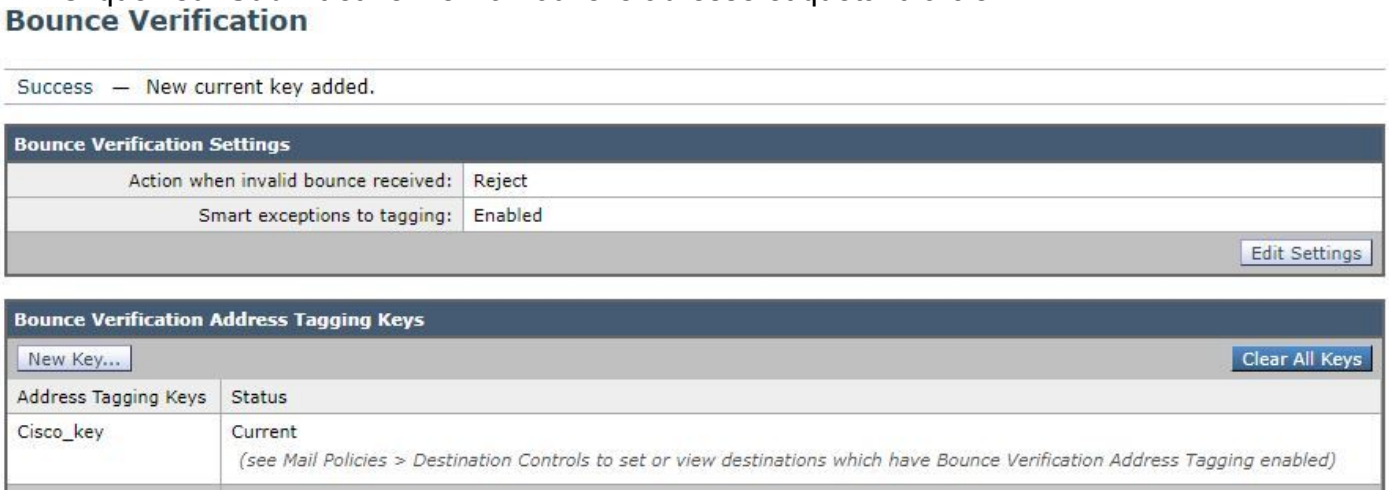
- Naviguez **pour envoyer par mail des stratégies > la vérification de rebond** et pour cliquer sur New la **clé**



- Entrez dans n'importe quel texte arbitraire à utiliser comme clé pour le codage et décoder des balises d'adresse. Par exemple, « Cisco_key ».

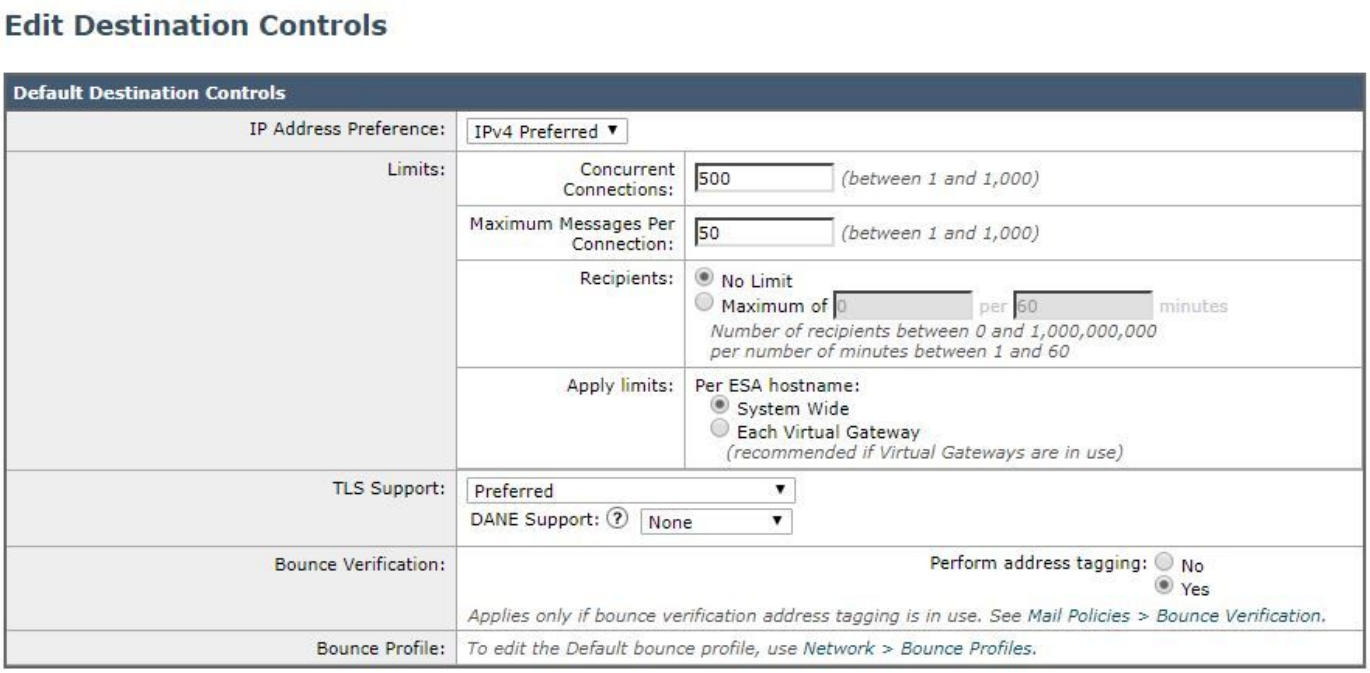


- Cliquez sur Submit et vérifiez la nouvelle adresse étiquetant la clé

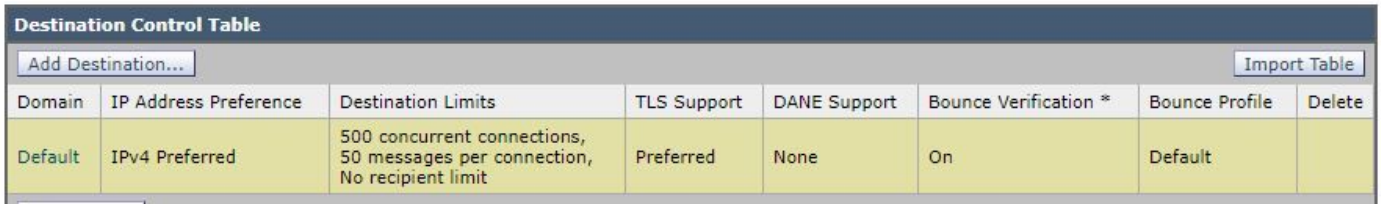


Maintenant, activons la vérification de rebond pour notre domaine « par défaut » :

- Naviguez **pour envoyer par mail des stratégies > des contrôles de destination** et pour cliquer sur en fonction le **par défaut.**
- Configurez la **vérification de rebond : Exécutez l'étiquetage d'adresse : Oui**



- Cliquez sur Submit et **commettez les modifications.** Notez que la vérification de rebond est maintenant en fonction pour le domaine par défaut.



Utilisant le Tableau de contrôle de destination

La livraison incontrôlée d'email peut accabler les domaines réceptifs. L'ESA te donne le plein contrôle de la livraison de message en définissant le nombre de connexions que votre appliance s'ouvrira ou nombre de messages votre appliance enverra à chaque domaine de destination. La table de contrôles de destination fournit des configurations pour des débits de connexion et de message quand l'ESA livre aux destinations distantes. Il fournit également des configurations pour tenter ou imposer l'utilisation du TLS à ces destinations. L'ESA est configuré avec une configuration par défaut pour le Tableau de contrôle de destination.

Ce que nous couvrirons dans ce document est comment nous pouvons gérer et configurer le contrôle des destinations où le par défaut n'est pas une adaptation. Par exemple, Google a un ensemble de réception ordonne que les utilisateurs de Gmail devraient suivre ou ils risquent d'envoyer soutiennent un code de réponse du SMTP 4XX et un message vous indiquant envoient trop rapidement, ou la boîte aux lettres du destinataire a dépassé sa limite de mémoire. Nous ajouterons le domaine de Gmail à la table de contrôle de destination limitant la quantité de message envoyée à un destinataire de Gmail ci-dessous.

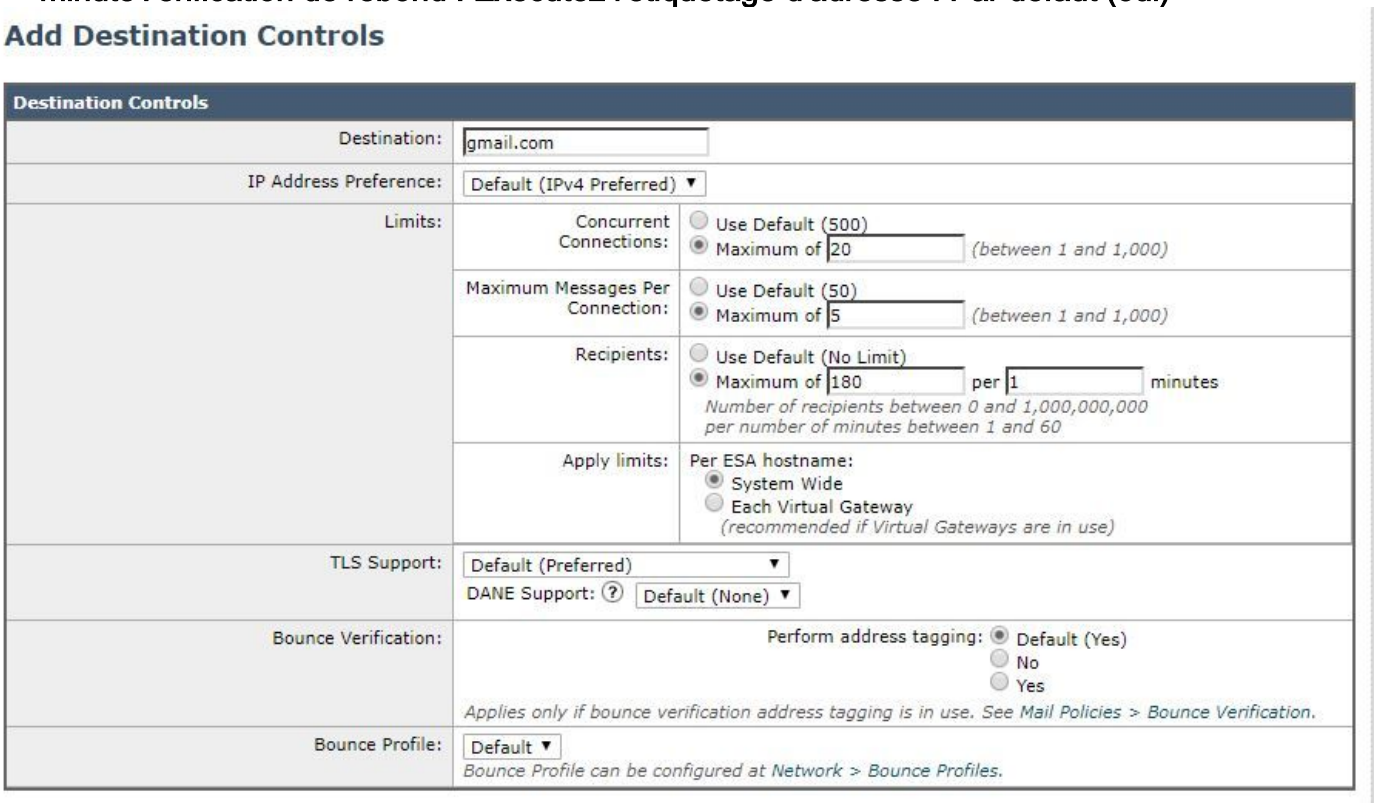
Ajouter un nouveau domaine au Tableau de contrôle de destination

Comme mentionné, Google a des limites pour des expéditeurs envoyant à Gmail. La réception des limites peut être vérifiée en regardant l'expéditeur de Gmail - https://support.google.com/a/answer/1366776?hl=en ici édité par limites

Installons le domaine de destination pour Gmail comme un exemple de bonnes stratégies

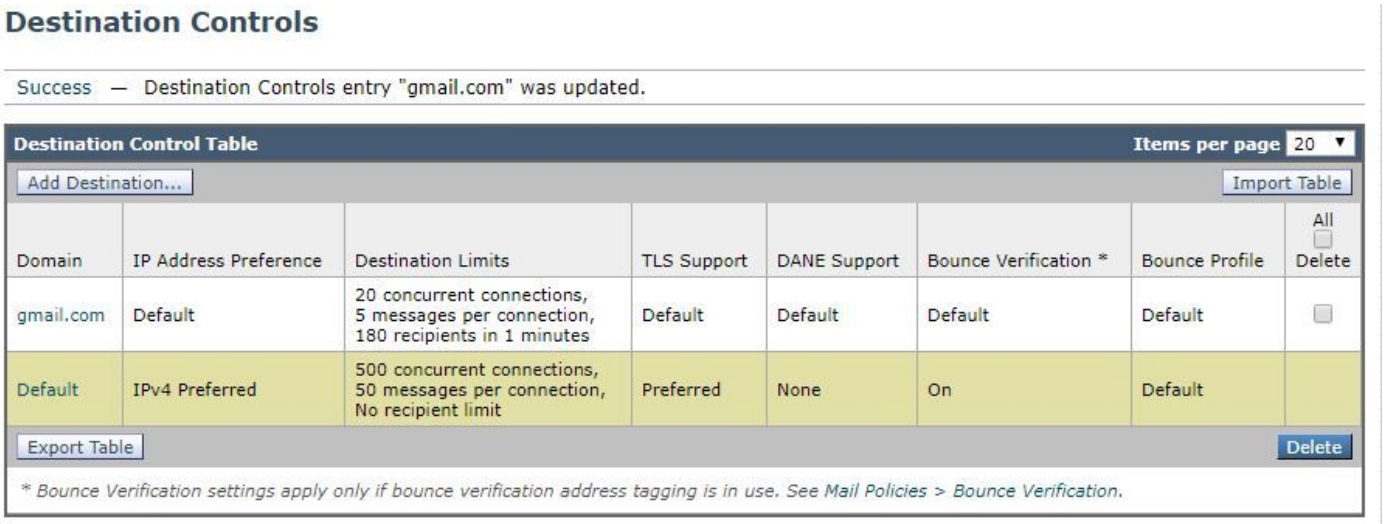
voisines.

- Naviguez **pour envoyer par mail des stratégies > des contrôles de destination** et pour cliquer sur Add la **destination** et pour créer un nouveau profil utilisant les paramètres suivants : **Destination : gmail.comPréférence d'adresse IP : Ipv4 préféréConnexions simultanées : Maximum de 20Messages maximum par connexion : 5Destinataires : Maximum de 180 par 1 minuteVérification de rebond : Exécutez l'étiquetage d'adresse : Par défaut (oui)**



- Cliquez sur Submit et **commettez les modifications.** C'est ce qui ressemble à notre Tableau de contrôle de destination après l'ajout du domaine.

La note « destination limite » et la « vérification de rebond » change dans l'image ci-dessous :



Déployant l'authentification basée sur dn de SMTP Désignée d'Entities (DANOIS)

L'authentification basée sur dn de SMTP du protocole Désigné d'Entities (DANOIS) valide vos Certificats X.509 avec des noms DNS utilisant une extension du degré de sécurité de système de noms de domaine (DNSSEC) configurée sur votre serveur DNS et un enregistrement de ressource en DN, également connu sous le nom d'enregistrement TLSA.

L'enregistrement TLSA est ajouté dans le certificat qui contient des détails au sujet de l'Autorité de certification (CA), du certificat de fin-entité, ou de l'ancre de confiance utilisée pour le nom DNS décrit dans RFC 6698. Les extensions du degré de sécurité de système de noms de domaine (DNSSEC) fournissent la Sécurité ajoutée sur les DN en adressant des vulnérabilités dans le degré de sécurité de DN. DNSSEC utilisant des clés cryptographiques et des signatures numériques s'assure que les données de consultation sont correctes et se connecte pour légitimer des serveurs.

Ce qui suit sont les avantages d'utiliser le DANOIS de SMTP pour les connexions sortantes de TLS :

- Fournit la livraison sécurisée des messages des attaques en empêchant des attaques du downgrade (MITM), l'écoute illicite et empoisonnement Homme-dans-le-moyens de cache DNS.
- Fournit l'authenticité des Certificats et de l'information DNS de TLS, une fois sécurisé par DNSSEC.

Configuration ESA

Avant que vous commenciez le DANOIS d'établissement sur l'ESA, assurez-vous s'il vous plaît que l'expéditeur d'enveloppe et l'enregistrement de ressource TLSA est DNSSEC vérifié et que le domaine de réception est DANOIS protégé. Vous pouvez faire ceci sur l'ESA utilisant la commande CLI **daneverify**.

- Naviguez **pour envoyer par mail des stratégies > des contrôles de destination** et pour cliquer sur Add la **destination** et pour créer un nouveau profil utilisant les paramètres suivants : **Destination : dane_protected.comSupport de TLS :** Préféré**Support de DANOIS :** Opportuniste

Add Destination Controls

Destination Controls		
Destination:	dane_protected.com	
IP Address Preference:	Default (IPv4 Preferred) ▼	
Limits:	Concurrent Connections:	○ Use Default (500) ◉ Maximum of 500 *(between 1 and 1,000)*
	Maximum Messages Per Connection:	○ Use Default (50) ◉ Maximum of 50 *(between 1 and 1,000)*
	Recipients:	◉ Use Default (No Limit) ○ Maximum of 0 per 60 minutes *Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60*
	Apply limits:	Per ESA hostname: ◉ System Wide ○ Each Virtual Gateway *(recommended if Virtual Gateways are in use)*
TLS Support:	Preferred ▼ DANE Support: ? Opportunistic ▼	
Bounce Verification:	Perform address tagging: ◉ Default (Yes) ○ No ○ Yes *Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.*	
Bounce Profile:	Default ▼ *Bounce Profile can be configured at Network > Bounce Profiles.*	

- Cliquez sur Submit et **commettez les modifications.**