Comprendre les paramètres liés aux stratégies de flux de courrier et aux contrôles de destination

Contenu

Introduction

Ce document décrit quelques aspects de configuration de l'ESA (Email Security Appliance) sur la façon de limiter les expéditeurs et la remise. Les fonctionnalités décrites dans cet article sont les stratégies de flux de messages et les contrôles de destination.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base des stratégies de flux de courrier et des contrôles de destination
- Connaissance de l'utilisation de ces fonctions dans la configuration du ESA

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Avantages des stratégies de flux de courrier et des contrôles de destination

Ces deux fonctionnalités ont une fonction très importante, à savoir la limitation/limitation de débit. Cet aspect aide l'administrateur à contrôler quel trafic doit circuler librement et quel trafic doit être autorisé avec des restrictions.

Stratégies de flux de messages

Il s'agit des politiques qui s'appliquent aux groupes d'expéditeurs de l'ESA, sur la base desquelles la modulation du trafic de messagerie électronique est effectuée.

Les stratégies de flux de messages s'appliquent toujours au trafic entrant dans le ESA, indépendamment du fait que le courrier électronique soit entrant ou sortant.

Les stratégies de flux de messages fonctionnent dans le serveur principal en ce qui concerne le comportement de connexion sélectionné pour cette stratégie. Les différents comportements de connexion disponibles dans les ESA sont les suivants :

1. Accept (accepter)
2. Rejeter
3. Relais
4. Refus TCP
5. Continuer

Accept (accepter): La connexion est acceptée et l'acceptation des e-mails est ensuite limitée par les paramètres de l'écouteur, y compris la table d'accès aux destinataires (pour les auditeurs publics). Ce comportement de connexion traite un e-mail comme entrant

Rejeter : Le client qui tente de se connecter obtient un code d'état SMTP 4XX ou 5XX. Aucun e-mail n'est accepté. Il est principalement utilisé pour les expéditeurs de listes noires

Relais : La connexion est acceptée. La réception d'un destinataire est autorisée et n'est pas limitée par la table d'accès des destinataires. Ceci traite un e-mail comme sortant

Refus TCP : La connexion est refusée au niveau TCP.

Continuer : Le mappage dans le TAH est ignoré et le traitement du TAH se poursuit. Si la connexion entrante correspond à une entrée ultérieure qui n'est pas CONTINUE, cette entrée est utilisée à la place. La règle CONTINUE est utilisée pour faciliter la modification du TAH dans l'interface utilisateur graphique.

Composants d'une stratégie de flux de courrier

Maximum. Messages par connexion : Nombre maximal de messages pouvant être envoyés via cet écouteur par connexion à partir d'un hôte distant. Chaque ICID représente une connexion

Maximum. Destinataires par message : Nombre maximal de destinataires par message qui seront acceptés à partir de cet hôte et qui seront traités à l'aide de cette stratégie de flux de messages

Maximum. Taille du message : Taille maximale d'un message qui sera accepté par cet écouteur marqué dans la stratégie de flux de messages. La taille maximale de message la plus petite possible est de 1 kilo-octet.

Maximum. Connexions simultanées à partir d'une seule adresse IP : Nombre maximal de connexions simultanées autorisées à se connecter à cet écouteur à partir d'une adresse IP unique.

Code de bannière SMTP personnalisé : Le code SMTP retourné lorsqu'une connexion est établie avec cet écouteur.

Texte de la bannière SMTP personnalisée : Le texte de la bannière SMTP retourné lorsqu'une connexion est établie avec cet écouteur. Vous pouvez utiliser certaines variables dans ce champ.

Remplacer le nom d'hôte de la bannière SMTP : par défaut, l'appliance inclut le nom d'hôte associé à l'interface du processus d'écoute lors de l'affichage de la bannière SMTP aux hôtes distants (par exemple, ESMTP, 220 noms d'hôte). Vous pouvez choisir de remplacer cette bannière en entrant un autre nom d'hôte ici. En outre, vous pouvez laisser le champ hostname vide pour choisir de *ne pas* afficher un nom d'hôte dans la bannière.

Limites de flux de courrier

Maximum. Destinataires par heure : Nombre maximal de destinataires par heure que cet écouteur recevra d'un hôte distant. Le nombre de destinataires par adresse IP de l'expéditeur est suivi globalement. Cependant, chaque écouteur suit son propre seuil de limitation de débit, car tous les écouteurs se valident sur un seul compteur, il est plus probable que la limite de débit soit dépassée si la même adresse IP (expéditeur) se connecte à plusieurs écouteurs. Vous pouvez utiliser certaines variables dans ce champ.

Maximum. Destinataires par heure Code : Code SMTP renvoyé lorsqu'un hôte dépasse le nombre maximal de destinataires par heure défini pour cet écouteur.

Maximum. Destinataires par heure Texte : Le texte de la bannière SMTP renvoyé lorsqu'un hôte dépasse le nombre maximal de destinataires par heure défini pour cet écouteur.

Limite de débit pour les expéditeurs de messages

Maximum. Destinataires par intervalle de temps : Nombre maximal de destinataires pendant une période spécifiée que cet écouteur recevra d'un expéditeur d'enveloppe unique, en fonction de l'adresse de courrier. Le nombre de destinataires est suivi globalement. Chaque auditeur suit son propre seuil de limitation de débit ; cependant, comme tous les écouteurs se valident sur un seul compteur, il est plus probable que la limite de débit sera dépassée si les messages de la même adresse de courrier sont reçus par plusieurs écouteurs.

Code d'erreur de limite de débit de l'expéditeur : Code SMTP renvoyé lorsqu'une enveloppe

dépasse le nombre maximal de destinataires pour l'intervalle de temps défini pour cet écouteur.

Texte d'erreur de limite de débit de l'expéditeur : Le texte de la bannière SMTP renvoyé lorsqu'un expéditeur d'enveloppe dépasse le nombre maximal de destinataires pour l'intervalle de temps défini pour cet écouteur.

Exceptions : Si vous souhaitez que certains expéditeurs d'enveloppes soient exemptés de la limite de taux définie, sélectionnez une liste d'adresses contenant les expéditeurs d'enveloppes.

La liste d'adresses est définie dans Politiques de messagerie à Liste d'adresses (les adresses de messagerie complètes, les domaines et les adresses IP peuvent être utilisés pour les exemptions).

Utiliser SenderBase pour le contrôle de flux : Activez “ recherches ” au service de réputation SenderBase pour cet écouteur.

Regrouper par similarité des adresses IP : Utilisé pour suivre et évaluer la limite des messages entrants par adresse IP lors de la gestion des entrées dans la table d'accès hôte (HAT) d'un écouteur dans de grands blocs CIDR. Vous définissez une plage de bits significatifs (de 0 à 32) par lesquels regrouper des adresses IP similaires aux fins de limitation de débit, tout en conservant un compteur individuel pour chaque adresse IP de cette plage.

NOTE: Nécessite “'utiliser SenderBase ” pour être désactivé.

DHAP (Directory Harvest Attack Prevention)

Maximum. Destinataires non valides par heure : Nombre maximal de destinataires non valides par heure que cet écouteur recevra d'un hôte distant. Ce seuil représente le nombre total de refus RAT et de refus du serveur SMTP Call-Advance combinés au nombre total de messages destinés à des destinataires LDAP non valides abandonnés dans la conversation SMTP ou renvoyés dans la file d'attente de travail (tel que configuré dans les paramètres d'acceptation LDAP sur l'écouteur associé).

Supprimer la connexion si le seuil DHAP est atteint dans une conversation SMTP :

La solution matérielle-logicielle abandonne une connexion à un hôte si le seuil des destinataires non valides est atteint.

Maximum. Code Destinataires Par Heure Non Valide : Spécifiez le code à utiliser lors de la suppression des connexions. Le code par défaut est 550.

Maximum. Texte Destinataires non valides par heure : Spécifiez le texte à utiliser pour les connexions abandonnées. Le texte par défaut est “ Trop de destinataires non valides.

Fonctions de sécurité

Vérification de la réputation des spams/AMP/virus/expéditeurs/filtres contre les attaques / protection avancée contre les hameçonnages / filtres de courriers indésirables / contenus et messages : L'analyse associée aux moteurs/analyses de sécurité et aux filtres peut être activée ou désactivée à partir d'ici

Chiffrement et authentification : Nous pouvons modifier les paramètres comme Désactivé, Préféré ou Exiger la sécurité de la couche de transport (TLS) dans les conversations SMTP de cet écouteur.

L'option Vérifier le certificat client demande au dispositif de sécurité de la messagerie d'établir une connexion TLS à l'application de messagerie de l'utilisateur si le certificat client est valide.

Pour le TLS Preferred, l'appliance autorise toujours une connexion non TLS si l'utilisateur n'a pas de certificat, mais refuse une connexion si l'utilisateur a un certificat non valide.

Pour le paramètre TLS Required, la sélection de cette option nécessite que l'utilisateur dispose d'un certificat valide pour que l'appliance autorise la connexion.

Authentification SMTP : Autorise, désautorise ou nécessite l'authentification SMTP des hôtes distants se connectant au processus d'écoute

Si l'authentification TLS et SMTP est activée : Exiger TLS pour offrir l'authentification SMTP

Signature de clé de domaine/DKIM : Activer la signature des clés de domaine ou DKIM sur cet écouteur

Vérification DKIM : Activez la vérification DKIM.

Décryptage/vérification S/MIME : Activez le déchiffrement ou la vérification S/MIME.

Signature après traitement : Choisissez de conserver ou de supprimer la signature numérique des messages après la vérification S/MIME.

Récupération de clé publique S/MIME : Activez la collecte des clés publiques S/MIME.

Récupérer les certificats en cas d'échec de vérification : Indiquez si vous voulez récupérer les clés publiques si la vérification des messages signés entrants échoue.

Enregistrer le certificat mis à jour : Choisir s'il faut récolter les clés publiques mises à jour

Vérification SPF/SIDF : Activez la signature SPF/SIDF sur cet écouteur.

Niveau de conformité : Définissez le niveau de conformité SPF/SIDF. Vous pouvez choisir entre SPF, SIDF ou SIDF Compatible

Rétrograder le résultat de la vérification PRA si 'Resent-Sender:' ou 'Resent-From:' ont été utilisés : Si vous choisissez un niveau de conformité compatible SIDF, configurez si vous voulez rétrograder le résultat de la vérification de l'identité PRA à Aucun s'il y a Rent-Sender : ou Rent-De : en-têtes présents dans le message

Test HELO : Configurez si vous souhaitez effectuer un test sur l'identité HELO (utilisez cette option pour les niveaux de conformité compatibles SPF et SIDF).

Vérification DMARC : Activer la vérification DMARC sur cet écouteur

Utiliser le profil de vérification DMARC : Sélectionnez le profil de vérification DMARC que vous voulez utiliser sur cet écouteur. La même chose est créée à partir des stratégies de messagerie

—> DMARC —> Ajouter un profil

Rapports de commentaires DMARC : Activez l'envoi de rapports de commentaires agrégés DMARC.

Vérification du renvoi

Considérez les renvois non étiquetés comme valides : S'applique uniquement si l'étiquetage de vérification de renvoi est activé. Par défaut, la solution matérielle-logicielle considère les rebondissements non étiquetés comme non valides et rejette le renvoi ou ajoute un en-tête personnalisé, selon les paramètres de vérification du renvoi. Si vous choisissez de considérer les rebondissements non étiquetés comme valides, l'appliance accepte le message de renvoi.

Vérification de l'expéditeur

Vérification DNS de l'expéditeur du message :

Les expéditeurs peuvent être non vérifiés pour différentes raisons. Les expéditeurs non vérifiés sont classés dans les catégories suivantes :

- L'enregistrement PTR de l'hôte de connexion n'existe pas dans le DNS.
- Échec de la recherche d'enregistrement PTR de l'hôte en raison d'une défaillance DNS temporaire.
- La recherche DNS inverse de l'hôte de connexion (PTR) ne correspond pas à la recherche DNS directe (A).

Nous pouvons activer ou désactiver la fonction Vérification de l'expéditeur.

Utiliser la table des exceptions de vérification de l'expéditeur : Nous pouvons utiliser la table d'exceptions du domaine de vérification de l'expéditeur pour autoriser les exemptions. Nous ne pouvons avoir qu'une seule table d'exceptions, mais peut être activée par stratégie de flux de courrier.

La table Exception peut être créée à partir des stratégies de messagerie —> Table des exceptions de vérification de l'expéditeur —> Ajouter une exception de vérification de l'expéditeur

Contrôles de destination

Il s'agit d'une fonctionnalité qui contrôle les livraisons de courrier électronique. Tous les e-mails qui terminent le traitement via les ESA et qui sont sur le point de quitter les ESA pour d'autres livraisons peuvent être contrôlés par la fonction Contrôles de destination.

Le profil **Default** Destination Controls s'applique à toutes les livraisons. Au cas où des contrôles de livraison spécifiques à un domaine sont nécessaires, nous devons créer un profil de contrôle de destination personnalisé.

Composants d'un profil de contrôles de destination

Limites

Connexions simultanées : Nombre de connexions simultanées (DCID) aux hôtes distants que l'appliance tente d'ouvrir pour terminer la livraison.

Nombre maximal de messages par connexion : Nombre de messages que l'ESA enverra à un domaine de destination via une connexion (DCID) avant que l'appliance n'initie une nouvelle connexion.

Destinataires : Nombre de destinataires que l'appliance enverra à un hôte distant donné au cours d'une période donnée.

Appliquer les limites : Ces aspects permettent de décider comment appliquer les limites que nous avons spécifiées pour chaque destination et par nom d'hôte MGA.

Prise en charge TLS

Cela permet de décider si les connexions TLS aux hôtes distants seront définies sur Aucun / Préféré / Obligatoire

Support DANE : Si vous configurez DANE comme 'Opportuniste' et que l'hôte distant ne prend pas en charge DANE, TLS opportuniste est préférable pour le chiffrement des conversations SMTP.

Si vous configurez DANE comme étant obligatoire et que l'hôte distant ne prend pas en charge DANE, aucune connexion n'est établie à l'hôte de destination.

Si vous configurez DANE comme 'Obligatoire' ou 'Opportuniste' et que l'hôte distant prend en charge DANE, il est préférable pour le chiffrement des conversations SMTP.

NOTE: DANE ne sera pas appliqué aux domaines dont les routes SMTP sont configurées.

Vérification du renvoi

Cela permet de décider si l'étiquetage de l'adresse de l'expéditeur de l'enveloppe (prvs-xxxxxx-xxxx) doit être effectué ou non via la vérification du renvoi.

La vérification du renvoi peut être configurée à partir des stratégies de messagerie —> Vérification du renvoi —> Ajouter une nouvelle clé

Profil de renvoi

Le profil de renvoi peut être utilisé par la solution matérielle-logicielle pour un hôte distant donné. Il décide de la durée de conservation d'un e-mail dans la file d'attente de livraison de l'ESA en cas de problème de livraison, avant le renvoi d'un e-mail sur papier

Le profil de renvoi est défini via le réseau —> Profils de renvoi

Paramètres globaux

Certificat: Il s'agit de l'aspect dans lequel nous définissons les certificats qui doivent être utilisés lors de l'établissement de connexions SSL/TLS lors de l'envoi de messages électroniques au

prochain saut. Il est toujours recommandé d'utiliser un certificat signé par une autorité de certification (AC) dans cet aspect.

Envoyer une alerte en cas d'échec d'une connexion TLS requise : Nous pouvons spécifier si l'appliance envoie une alerte si la négociation TLS échoue lors de la remise de messages à un domaine qui nécessite une connexion TLS. Le message d'alerte contient le nom du domaine de destination pour la négociation TLS ayant échoué. L'appliance envoie le message d'alerte à tous les destinataires définis pour recevoir les alertes de niveau de gravité **Avertissement** pour les types **d'alerte système**.

Nous pouvons gérer les destinataires des alertes via Administration système —> Alertes