Pratiques recommandées de configuration pour le CES ESA

Contenu

Introduction

Ce document fournit un résumé des recommandations pour des administrateurs employant la sécurité du courrier électronique du nuage de Cisco (CES) pour configurer leur appliance de sécurité du courrier électronique de Cisco (ESA).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Gestion ESA, gestion de niveau CLI et GUI

Composants utilisés

Les informations dans ce document sont basées sur des pratiques recommandées et des recommandations pour des clients et des administrateurs de CES.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-

vous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

Ce document peut également être utilisé avec les versions de matériel et de logiciel suivantes :

- Matériel de sur-sites ESA et appliances virtuelles (non-CES) exécutant toute version d'AsyncOS pour la sécurité du courrier électronique

Pratiques recommandées de configuration pour le CES ESA

> **Avertissement** : Tous les changements à la configuration fondée sur les pratiques recommandées de la manière prévue de ce document devraient être passés en revue et compris avant de commettre vos changements de configuration d'un environnement de production. Consultez s'il vous plaît votre ingénieur système ou équipe chargée du compte de CES avant d'apporter les modifications de configuration avec lesquelles vous 100% ne comprenez pas ou avez le confort en administrant.

Services de sécurité

Anti-Spam d'IronPort (IPAS)

- Toujours le Mo du balayage 1.5 et ne balayent jamais 2 Mo

Filtrage des URL

- Catégorisation et réputation URL d'enable
- Cheminement d'interaction de Web d'enable

Détection de Graymail

- Mo de la taille 1 de messages d'enable et de maximum

Filtres d'épidémie

- Activez les règles adaptatives, Mo maximum de la taille 1 de balayage
- Cheminement d'interaction de Web d'enable

Protection avancée de malware

- Types de fichier supplémentaires d'enable après l'activation de la caractéristique

Cheminement de message

- Se connecter de connexion rejeté par enable (s'il y a lieu)

Administration système

Utilisateurs

- Stratégies de set password
- Si possible accroissez le Protocole LDAP (Lightweight Directory Access Protocol) pour

l'authentification

Abonnements de log

- Logs d'historique de configuration d'enable
- Logs de Filtrage URL d'enable
- En-tête supplémentaire de log « de »

Modifications de niveau CLI

Filtrage URL de la sécurité Web SDS

- **websecurityadvancedconfig**

```
Do you want to disable DNS lookups? [N]> y

Enter the maximum number of URLs that should be scanned:
[100]> 20

Enter the threshold value for outstanding requests:
[50]> 5

Enter the default time-to-live value (seconds):
[30]> 600

Do you want to rewrite all URLs with secure proxy URLs? [Y]> n
```

Se connecter URL

- ESA activant le Filtrage URL et les pratiques recommandées
- **outbreakconfig**

```
Logging of URLs is currently disabled.

Do you wish to enable logging of URL's? [N]> y

Logging of URLs has been enabled.
```

Anti-charriez le filtre

- Détection modifiée d'email (ALIMENTÉE) avec la sécurité du courrier électronique de Cisco

En-tête emboutissant le filtre

- écrivez et activez le filtre de message suivant :

```
addHeaders:  if (sendergroup != "RELAYLIST")
{
    insert-header("X-IronPort-RemoteIP", "$RemoteIP");
    insert-header("X-IronPort-MID", "$MID");
    insert-header("X-IronPort-Reputation", "$Reputation");
    insert-header("X-IronPort-Listener", "$RecvListener");
    insert-header("X-IronPort-SenderGroup", "$Group");
    insert-header("X-IronPort-MailFlowPolicy", "$Policy");
}
```

Tableau d'accès au hôte

Groupes supplémentaires d'expéditeur

- Guide utilisateur ESA : Création d'un groupe d'expéditeur pour la gestion de messages SKIP_SBRS – Endroit plus élevé pour les sources qui ignorent la réputationSPOOF_ALLOW – Une partie de filtre de mystificationPARTENAIRE – Pour le TLS connexions forcées

Dans le groupe d'expéditeur des prédéfinis SUSPECTLIST

- Guide utilisateur ESA : Vérification d'expéditeur : Hôte enable « scores SBRS sur aucun »Sur option, l'enable « connecter consultation d'enregistrement PTR d'hôte échoue en raison de la panne provisoire de DN »

Échantillon agressif de CHAPEAU

- LISTE NOIRE [-10 à la STRATÉGIE -2] : BLOQUÉ
- SUSPECTLIST [-2 à la STRATÉGIE -1] : HEAVYTHROTTLED
- GRAYLIST[-1 à 2 et AUCUN] STRATÉGIE : LIGHTTHROTTLED
- ACCEPTLIST [2 à la STRATÉGIE 10] : REÇU

> Remarque: Les exemples ci-dessus de CHAPEAU affichent des stratégies supplémentaire configurées de flux de courrier. Pour des informations complètes sur MFP, référez-vous s'il vous plaît au guide utilisateur de la version appropriée d'AsyncOS pour l'exécution de sécurité du courrier électronique sur votre ESA. Exemple, AsyncOS 10.0 : Tableau d'accès au hôte (CHAPEAU), groupes d'expéditeur, et stratégies de flux de courrier

Stratégie de flux de courrier (paramètres de stratégie par défaut)

Paramètres de sécurité

- Placez le Transport Layer Security (TLS) à préférer
- Enable Sender Policy Framework (SPF)
- Messagerie identifiée par DomainKeys d'enable (DKIM)
- Activez l'authentification de message basée sur domaine, l'enregistrement et la vérification de la conformité (DMARC) et envoyez les rapports des commentaires d'agrégat

> Remarque: DMARC exige l'accord supplémentaire à configurer. Pour des informations complètes sur DMARC, référez-vous s'il vous plaît au guide utilisateur de la version appropriée d'AsyncOS pour l'exécution de sécurité du courrier électronique sur votre ESA. Exemple, AsyncOS 10.0 : Vérification DMARC

Stratégies de messagerie entrante

Seuils d'anti-Spam

- Des seuils devraient être laissés aux seuils par défaut. La modification du marquage a pu avoir comme conséquence une augmentation de faux positif.

Antivirus

- Lecture de message : Balayage pour des virus seulement
- Les messages d'Unscannable, virus ont infecté des messages : placez le « premier message d'archives » à l'aucun

AMPÈRE

- Ajoutez le « AMPÈRE » pour soumettre ajoutent au début pour Unscannable, débronchement « message d'archives »

Graymail

- La lecture activée pour chaque verdict, ajoutent le sujet et le livrent au début
- Ajoutez la x-en-tête pour l'email en vrac, en-tête = « X-BulkMail », valeur = « vrai »

Filtres d'épidémie

- Le niveau par défaut de menace est 3, s'ajustent s'il vous plaît selon vos exigences de sécurité Si le niveau de menace pour un message égale ou dépasse ce seuil, le message sera envoyé à la quarantaine d'épidémie. (menace 1=lowest, menace 5=highest)
- Modification de message d'enable. URL de réécriture pour le message non signé
- Le sujet de modification ajoutent au début à : [Fraude possible $threat_category]

Stratégies de mail sortant

Antivirus

- Lecture de message
- Balayage pour des virus seulementl'ONU-contrôle incluent une X-en-tête avec les résultats de lecture poids du commerce dans le message
- Pour tous les messages : Avancé > l'autre notification, enable « d'autres » et incluent l'adresse e-mail de contact admin/SOC

Quarantaines de stratégie

Pré-créez les quarantaines suivantes :

- D'arrivée inadéquat
- Sortant inadéquat
- D'arrivée malveillant URL
- Sortant malveillant URL
- Le suspect charrient
- Malware

D'autres configurations

Dictionnaires

- Enable/blasphème d'examen et dictionnaire sexuel de termes
- Créez le dictionnaire modifié d'email avec les noms exécutifs
- Créez le dictionnaire pour mots clé restreints ou autres

Contrôles de destination

- TLS d'enable pour la destination par défaut
- Placez les seuils inférieurs pour des domaines de webmail
- Raté limit votre propre messagerie sortante avec des configurations de contrôle de destination

Filtres satisfaits

> Remarque: Pour des informations complètes sur les filtres satisfaits, référez-vous s'il vous plaît au guide utilisateur de la version appropriée d'AsyncOS pour l'exécution de sécurité du courrier électronique sur votre ESA. Exemple, AsyncOS 10.0 : Filtres satisfaits

Filtre de contenu inapproprié

- Le blasphème de conditions OU la correspondance de dictionnaire sexuelle, envoient une copie à la quarantaine inadéquate

Filtre malveillant de contenu de réputation URL

- Envoyez une copie à l'URL malveillant (-10 à -6) pour mettre en quarantaine

Filtre de contenu de catégorie URL avec ces derniers sélectionnés

- Adulte, pornographie, mauvais traitement à enfant, jouant
- Envoyez une copie à la quarantaine inadéquate

Détection modifiée d'email

- Nommé par dictionnaire « Executives_FED »
- Quarantaine du seuil 90 FED() une copie

La macro-instruction a activé le filtre satisfait de documents

- si un ou plusieurs connexions contiennent une macro-instruction
- État facultatif - > de plage non approuvée SBRS
- Envoyez une copie pour mettre en quarantaine

Protection de connexion

- si un ou plusieurs connexions sont protégées
- État facultatif - > de plage non approuvée SBRS
- Envoyez une copie pour mettre en quarantaine

Informations connexes

- BRKSEC-2131 - Sécurité du courrier électronique de Cisco : Pratiques recommandées et réglage fin (2016 Las Vegas)
- BRKSEC-2131 - Sécurité de courrier électronique pour des personnes de Non-E-messagerie (2015 San Diego)
- BRKSEC-3770 - (DMARC) - ne sont pas des phish : plongée en eau profonde dans des techniques d'authentification de courrier électronique (2014 San Francisco)
- Contrat de licence utilisateur final de CES
- Description de service de CES
- Termes universels de nuage de Cisco
- Support et documentation techniques - Cisco Systems