Qu'est-ce que le serveur agrégateur Cisco dans la messagerie sécurisée ?

Contenu

Introduction

Ce document décrit ce qu'est le serveur agrégateur Cisco et comment il fonctionne lorsque la passerelle de messagerie sécurisée interroge le serveur agrégateur Cisco (port agrégateur.cisco.com 443) toutes les 30 minutes pour les données de suivi d'interaction Web.

Qu'est-ce que le serveur agrégateur Cisco et comment fonctionne-t-il ?

La passerelle de messagerie sécurisée interroge le serveur d'agrégation Cisco (port 443 de l'agrégation.cisco.com) toutes les 30 minutes pour les données de suivi d'interaction Web. Si cette option est activée dans les fonctions de déclenchement et de filtrage, le rapport Web Interaction Tracking affiche les données suivantes :

- Les principales URL malveillantes réécrites qui ont été cliquées. Liste des personnes qui ont cliqué sur les URL malveillantes.Horodatage du clic.Si l'URL a été réécrite par un filtre de stratégie ou d'attaque.Une action est effectuée lorsque l'URL a été cliquée : autoriser, bloquer ou inconnu.
- Les personnes ayant cliqué sur les URL malveillantes réécrites.
- Détails du suivi des interactions Web. Liste de toutes les URL redirigées et réécrites du cloud.Une action est effectuée lorsque l'URL a été cliquée : autoriser, bloquer ou inconnu.

Note: Pour que les détails de l'interaction Web s'affichent, assurez-vous de sélectionner **Politiques de messagerie entrante > Filtres d'attaque** afin de configurer un filtre d'attaque et d'activer la modification des messages et la réécriture des URL. Configurez un filtre de contenu avec l'action **Rediriger vers Cisco Security Proxy**.

Configurer le serveur agrégateur Cisco

```
> aggregatorconfig

Choose the operation you want to perform:

- EDIT - Edit aggregator configuration

- CLUSTERSET - Set how aggregator is configured in a cluster.

- CLUSTERSHOW - Display how aggregator is configured in a cluster.

[]> edit

Edit aggregator address:

[aggregator.cisco.com]>

Successfully changed aggregator address to : aggregator.cisco.com
```

Comment activer le suivi des interactions Web

Vous pouvez activer le suivi des interactions Web via deux configurations de fonctions différentes.

Filtres contre les attaques

Via l'interface utilisateur graphique :

1. Connectez-vous à l'interface utilisateur graphique de votre passerelle de messagerie sécurisée.
2. Passez le curseur sur **les services de sécurité**.
3. Cliquez sur **Filtres d'attaques**.
4. Cliquez sur **Modifier les paramètres globaux**.
5. Cochez la case **Activer les filtres contre les attaques**.
6. Cochez la case **Activer le suivi des interactions Web**.
7. Cliquez sur Submit.
8. Cliquez sur **Valider**.

Via l'interface de ligne de commande :

```
> outbreakconfig

Outbreak Filters: Disabled

Choose the operation you want to perform:

- SETUP - Change Outbreak Filters settings.

- CLUSTERSET - Set how the Outbreak Filters are configured in a cluster.

- CLUSTERSHOW - Display how the Outbreak Filters are configured in a cluster.

[]> setup

Outbreak Filters: Disabled

Would you like to use Outbreak Filters? [Y]>
```

```
Outbreak Filters enabled.

Outbreak Filter alerts are sent when Outbreak rules cross the threshold (go above or back down
below), meaning that new messages of certain types could be

quarantined or will no longer be quarantined, respectively.

Would you like to receive Outbreak Filter alerts? [N]> Y

What is the largest size message Outbreak Filters should scan?

[524288]>

Do you want to use adaptive rules to compute the threat level of messages? [N]> Y

Logging of URLs is currently disabled.

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

Logging of URLs has been enabled.

Web Interaction Tracking is currently disabled.

Do you wish to enable Web Interaction Tracking? [N]> Y

Web Interaction Tracking is enabled.

The Outbreak Filters feature is now globally enabled on the system.  You must use the
'policyconfig' command in the CLI or the Email Security Manager in

the GUI to enable Outbreak Filters for the desired Incoming and Outgoing Mail Policies.
```

Filtrage des URL

Via l'interface utilisateur graphique :

1. Connectez-vous à l'interface utilisateur graphique de votre passerelle de messagerie sécurisée.
2. Passez le curseur sur **les services de sécurité**.
3. Cliquez sur **Filtrage des URL**.
4. Cliquez sur **Modifier les paramètres globaux.**
5. Cochez la case **Activer la catégorie d'URL et les filtres de réputation**.
6. Cochez la case **Activer le suivi des interactions Web**.
7. Cliquez sur Submit.
8. Cliquez sur **Valider**.

Via l'interface de ligne de commande :

```
> websecurityconfig

Enable URL Filtering? [N]> Y

Do you wish to enable Web Interaction Tracking? [N]> Y

Web Interaction Tracking is enabled.

Do you want to add URLs to the allowed list using a URL list? [N]>
```

Suivi des interactions Web

Faits importants :

- Les modules de rapport ne sont pas renseignés, sauf si le suivi des interactions Web est activé.
- Le reporting n'est pas renseigné en temps réel, il interroge le serveur d'agrégation et obtient de nouvelles données toutes les 30 minutes.
- L'affichage d'un événement de clic dans le suivi peut prendre jusqu'à 2 heures.
- Des rapports sont disponibles pour les messages entrants et sortants.
- Les événements de clic d'URL ne sont signalés que si l'URL a été réécrite par un filtre de stratégie ou d'attaque.

Si vous utilisez Security Management Appliance (SMA) pour la création de rapports centralisés :

1. Connectez-vous à votre SMA.
2. Cliquez sur l'onglet **E-mail**.
3. Passez le curseur sur **Reporting**.
4. Cliquez sur **Suivi des interactions Web**.

Journalisation du connecteur cloud

Dans les versions plus récentes d'AsyncOS, la passerelle de messagerie sécurisée prend désormais en charge les journaux du connecteur cloud, un nouvel abonnement au journal qui contient le suivi des interactions Web à partir du serveur d'agrégation Cisco. Ceci a été ajouté pour aider à dépanner le suivi des interactions Web en cas de problème.

Via l'interface utilisateur graphique :

1. Connectez-vous à l'interface utilisateur de la passerelle de messagerie sécurisée.
2. Passez le curseur sur **Administration du système**.
3. Cliquez sur **Log Subscriptions**.

Via l'interface de ligne de commande :

```
>logconfig

Currently configured logs:

    Log Name            Log Type                          Retrieval           Interval

-------------------------------------------------------------------------------
1. LDAP_Debug          LDAP Debug Logs                   Manual Download     None
2. audit_logs          Audit Logs                        Manual Download     None
3. cloud_connector     Cloud Connector Logs              Manual Download     None
```

Dépannage

Problème

Impossible de se connecter au serveur agrégateur Cisco.

Solution

1. Envoyez une requête ping au nom d'hôte du serveur Cisco Aggregator à partir de la passerelle de messagerie sécurisée. Vous pouvez utiliser la commande **aggatorconfig** afin de trouver le nom d'hôte.
2. Vérifiez la connexion proxy configurée dans **Services de sécurité > Mises à jour de service**.
3. Vérifiez le pare-feu, les périphériques de sécurité et le réseau.

443	TCP	Sortie	aggregator.cisco.com	Accès au serveur Cisco Aggregator.

- Établissez une connexion Telnet avec le serveur agrégateur à partir de la passerelle de messagerie sécurisée : agrégateur telnet.cisco.com 443
- Exécutez une capture de paquets vers le serveur d'agrégation à partir de la passerelle de messagerie sécurisée affectée.

4. Vérifiez DNS, assurez-vous que le nom d'hôte du serveur est résolu sur la passerelle de messagerie sécurisée (exécutez-le sur la passerelle de messagerie sécurisée affectée : nslookup agrégator.cisco.com).

Problème

Impossible de récupérer les informations de suivi des interactions Web à partir du serveur agrégateur Cisco.

Solution

1. Vérifiez la connexion proxy configurée dans **Services de sécurité > Mises à jour de service**.
2. Vérifiez le pare-feu, les périphériques de sécurité et le réseau.

443	TCP	Sortie	aggregator.cisco.com	Accès au serveur Cisco Aggregator.

- Établissez une connexion Telnet avec le serveur agrégateur à partir de la passerelle de messagerie sécurisée : agrégateur telnet.cisco.com 443
- Exécutez une capture de paquets vers le serveur d'agrégation à partir de la passerelle de messagerie sécurisée affectée.

3. Vérifiez DNS, assurez-vous que le nom d'hôte du serveur est résolu sur l'appliance (exécutez-le sur la passerelle de messagerie sécurisée affectée : nslookup agrégator.cisco.com).

Informations connexes

- Guides de l'utilisateur final de la passerelle de messagerie sécurisée Cisco
- Notes de version de Cisco Secure Email Gateway
- **Support et documentation techniques - Cisco Systems**