Secure EmailのCisco Aggregator Serverとは何ですか。

内容

概要

このドキュメントでは、Secure EメールゲートウェイがWeb Interaction Tracking（Wインタラクショントラッキング）データに対して30分ごとにCisco AggregATOR Server（AGGREGATOR.CISCO.COMポート443）をポーリングする場合のCisco AggregATOR Serverの概要と動作について説明します。

Cisco Aggregator Serverとは何ですか。また、どのように動作するのですか。

Secure Eメールゲートウェイは、Webインタラクショントラッキングデータに対して30分ごとにCisco Aggregator Server（aggregator.cisco.comポート443）をポーリングします。アウトブレイクおよびフィルタリング機能で有効にすると、Webインタラクショントラッキングレポートに次のデータが表示されます。

- クリックされた書き換えられた悪意のあるURLのトップ。 悪意のあるURLをクリックしたユーザのリスト。クリックのタイムスタンプ。ポリシーまたはアウトブレイクフィルタによってURLが書き換えられた場合。URLがクリックされたときにアクションが実行されます：allow、block、またはunknown。
- 書き換えられた悪意のあるURLをクリックした上位の人々。
- Webインタラクショントラッキングの詳細。 リダイレクトおよび書き換えされたすべてのクラウドURLのリスト。URLがクリックされたときにアクションが実行されます：allow、block、またはunknown。

注：[Web Interaction Details]が表示されるようにするには、[Incoming Mail Policies] > [Outbreak Filters]を選択して、アウトブレイクフィルタを設定し、メッセージの変更とURLの書き換えを有効にします。[Redirect to **Cisco Security Proxy**]アクションを使用して**コンテンツフィルタを設定**します。

Cisco Aggregator Serverの設定

```
> 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
```

Webインタラクショントラッキングを有効にする方法

Webインタラクショントラッキングは、2つの異なる機能設定で有効にできます。

アウトブレイク フィルタ

GUIを使用：

1. Secure Email GatewayのGUIにログインします。
2. [セキュリティ・ サービス]にカーソルを合わせます。
3. [Outbreak Filters]をクリックします。
4. [Edit Global Settings] をクリックします。
5. [Enable Outbreak Filters]をオンにします。
6. [Web Interaction Tracking]をオンにします。
7. [Submit] をクリックします。
8. 「コミット」をクリックします。

CLIを使用：

```
> 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.
```

URL フィルタリング

GUIを使用：

1. Secure Email GatewayのGUIにログインします。
2. [セキュリティ・ サービス]にカーソルを合わせます。
3. [URL Filtering]をクリックします。
4. [Edit Global Settings] をクリックします。
5. [Enable URL Category and Reputation Filters]をオンにします。
6. [Web Interaction Tracking]をオンにします。
7. [Submit] をクリックします。
8. 「コミット」をクリックします。

CLIを使用：

```
> 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]>
```

Webインタラクショントラッキング

重要：

- レポートモジュールは、Webインタラクショントラッキングが有効でない限り入力されません。
- レポートはリアルタイムで入力されず、アグリゲータサーバをポーリングし、30分ごとに新しいデータを取得します。
- トラッキングでクリックイベントを表示するには、最大2時間かかることがあります。
- 着信および発信メッセージに関するレポートを利用できます。
- URLクリックイベントは、ポリシーまたはアウトブレイクフィルタによってURLが書き換えられた場合にのみ報告されます。

中央集中型レポート作成にセキュリティ管理アプライアンス(SMA)を使用する場合：

1. SMAにログインします。
2. [電子メール]タブ**をクリック**します。
3. [レポート]の上にホバー**を移動します**。
4. [Webインタラクション**トラッキング]をクリックします**。

クラウドコネクタのロギング

AsyncOSの最近のバージョンでは、Secure Email GatewayでCloud Connector Logsがサポートされるようになりました。これは、Cisco Aggregator ServerからのWeb Interaction Trackingを含む新しいログサブスクリプションです。これは、問題が発生した場合のWeb Interaction Trackingのトラブルシューティングに役立つように追加されました。

GUIを使用：

1. Secure Email Gateway GUIにログインします。
2. [システム管理]の上**にカーソルを移動します**。
3. [**Log Subscriptions**]を**クリックします**。

CLIを使用：

```
>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
```

トラブルシュート

問題

Cisco Aggregator Serverに接続できません。

解決方法

1. Secure Email GatewayからCisco Aggregator Serverのホスト名にpingを実行します。**aggregatorconfig**コマンドを使用**して**ホスト名を検索できます。
2. [セキュリティサービス] > [サービスの更新]で構成**されたプロキシ接続を確認してください**。
3. ファイアウォール、セキュリティデバイス、およびネットワークを確認します。

443	TCP	アウト	aggregator.cisco.com	Cisco Aggregatorサーバへのアクセス。

- Secure Emailゲートウェイからアグリゲータサーバに Telnet接続します。telnet aggregator.cisco.com 443
- 影響を受けるセキュアEメールゲートウェイからアグリゲータサーバへのパケットキャプチャを実行します。

4. [DNS]をオンにし、サーバのホスト名がSecure Email Gatewayで解決されることを確認します(該当するSecure Email Gatewayで次を実行します。nslookup aggregator.cisco.com)。

問題

Cisco Aggregator ServerからWebインタラクショントラッキング情報を取得できません。

解決方法

1. [**Security Services**] > [**Service Updates**]で設定されているプロキシ接続を確認します。
2. ファイアウォール、セキュリティデバイス、およびネットワークを確認します。

443	TCP	アウト	aggregator.cisco.com	Cisco Aggregatorサーバへのアクセス。

- Secure Emailゲートウェイからアグリゲータサーバに Telnet接続します。telnet aggregator.cisco.com 443
- 影響を受けるセキュアEメールゲートウェイからアグリゲータサーバへのパケットキャプチャを実行します。

3. DNSをチェックし、サーバのホスト名がアプライアンスで解決されることを確認します(該当するセキュアEメールゲートウェイで次のコマンドを実行します。nslookup aggregator.cisco.com)。

関連情報

- Cisco Secure Eメールゲートウェイエンドユーザガイド
- Cisco Secure Eメールゲートウェイリリースノート
- **テクニカル サポートとドキュメント – Cisco Systems**