What is the Cisco Aggregator Server in Secure Email?

Contents

Introduction

This document describes what the Cisco Aggregator Server is and how it works when the Secure Email Gateway polls the Cisco Aggregator Server (aggregator.cisco.com port 443) every 30 minutes for Web Interaction Tracking data.

What is the Cisco Aggregator Server and how does it work?

The Secure Email Gateway polls the Cisco Aggregator Server (aggregator.cisco.com port 443) every 30 minutes for Web Interaction Tracking data. If enabled in the Outbreak and Filtering features, the Web Interaction Tracking report shows this data:

- Top rewritten malicious URLs that were clicked. List of who clicked the malicious URLs.Timestamp of the click.If the URL was rewritten by a Policy or Outbreak filter.Action is taken when the URL was clicked: allow, block, or unknown.
- Top people who clicked on the rewritten malicious URLs.
- Web Interaction Tracking details. A list of all the cloud redirected and rewritten URLs.Action is taken when the URL was clicked: allow, block, or unknown.

Note: For the Web Interaction Details to show up, ensure to select **Incoming Mail Policies** > **Outbreak Filters** in order to configure an Outbreak filter and enable message modification and URL rewriting. Configure a content filter with the **Redirect to Cisco Security Proxy** action.

Configure the Cisco Aggregator Server

```
> 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
```

How to Enable Web Interaction Tracking

You can enable Web Interaction Tracking via two different feature configurations.

Outbreak Filters

Via the GUI:

1. Log into your Secure Email Gateway's GUI.
2. Hover over **Security Services**.
3. Click on **Outbreak Filters**.
4. Click **Edit Global Settings**.
5. Check **Enable Outbreak Filters**.
6. Check **Enable Web Interaction Tracking**.
7. Click **Submit**.
8. Click **Commit**.

Via the CLI:

```
> 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 Filtering

Via the GUI:

1. Log into your Secure Email Gateway's GUI.
2. Hover over **Security Services**.
3. Click on **URL Filtering**.
4. Click **Edit Global Settings.**
5. Check **Enable URL Category and Reputation Filters**.
6. Check **Enable Web Interaction Tracking**.
7. Click **Submit**.
8. Click **Commit**.

Via the CLI:

```
> 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 Interaction Tracking

Important facts:

- Reporting modules are not populated unless Web Interaction Tracking is enabled.
- Reporting is not populated in real-time, it polls the aggregator server and obtains new data

every 30 minutes.
- It may take up to 2 hours to see a click event in the tracking.
- Reports are available for incoming and outgoing messages.
- URL clicking events are reported only if the URL was rewritten by a Policy or Outbreak filter.

If you use Security Management Appliance (SMA) for centralized reporting:

1. Log in to your SMA.
2. Click the **Email** tab.
3. Hover over **Reporting**.
4. Click **Web Interaction Tracking**.

Cloud Connector Logging

In more recent versions of AsyncOS, the Secure Email Gateway now supports Cloud Connector Logs, a new log subscription that contains Web Interaction Tracking from the Cisco Aggregator Server. This was added to help troubleshoot Web Interaction Tracking if issues occur.

Via the GUI:

1. Log in to your Secure Email Gateway GUI.
2. Hover over **System Administration**.
3. Click **Log Subscriptions**.

Via the CLI:

```
>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
```

Troubleshoot

Issue

Unable to Connect to the Cisco Aggregator Server.

Solution

1. Ping the hostname of the Cisco Aggregator Server from the Secure Email Gateway. You can use the **aggregatorconfig** command in order to find the hostname.
2. Verify the proxy connection configured in **Security Services > Service Updates**.
3. Check the firewall, security devices, and network.

443 TCP Out aggregator.cisco.com Access to the Cisco Aggregator server.

- Telnet to the aggregator server from the Secure Email gateway: telnet aggregator.cisco.com 443

- Run a packet capture to the aggregator server from the affected Secure Email Gateway.

4. Check DNS, make sure the hostname of the server resolves on the Secure Email Gateway (Run this on the affected Secure Email Gateway: nslookup aggregator.cisco.com).

Issue

Unable to retrieve web interaction tracking information from the Cisco Aggregator Server.

Solution

1. Verify the proxy connection configured in **Security Services** > **Service Updates**.
2. Check the firewall, security devices, and network.

443	TCP	Out	aggregator.cisco.com	Access to the Cisco Aggregator server.

- Telnet to the aggregator server from the Secure Email gateway: telnet aggregator.cisco.com 443
- Run a packet capture to the aggregator server from the affected Secure Email Gateway.

3. Check DNS, make sure the hostname of the server resolves on the appliance (run this on the affected Secure Email Gateway: nslookup aggregator.cisco.com).

Related Information

- Cisco Secure Email Gateway End-User Guides
- Cisco Secure Email Gateway Release Notes
- **Technical Support & Documentation - Cisco Systems**