Secure Email中的Cisco Aggregator Server是什麼？

目錄

簡介

本檔案將說明思科聚合器伺服器是什麼，以及安全電子郵件閘道每30分鐘輪詢思科聚合器伺服器(aggregator.cisco.com連線埠443)以取得網路互動追蹤資料時其運作方式。

什麼是Cisco Aggregator Server？它如何工作？

安全電子郵件網關每30分鐘輪詢一次Cisco Aggregator Server(aggregator.cisco.com埠443)，以獲取網路互動跟蹤資料。如果在「爆發和過濾」功能中啟用，「Web Interaction Tracking」報告將顯示以下資料：

- 點選的重寫惡意網址最多。 按一下惡意URL的人員清單。按一下的時間戳。如果策略或爆發過濾器重寫了URL。按一下URL時執行的操作：allow、block或unknown。
- 點選重寫的惡意URL的頂級人員。
- Web互動跟蹤詳細資訊。 所有雲重定向和重寫URL的清單。按一下URL時執行的操作：allow、block或unknown。

附註：要顯示Web互動詳細資訊，請確保選擇**Incoming Mail Policies > Outbreak Filters**以配置爆發過濾器並啟用郵件修改和URL重寫。使用**Redirect to Cisco Security Proxy**操作配置內容過濾器。

配置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
```

如何啟用Web互動跟蹤

您可以通過兩種不同的功能配置啟用網路互動跟蹤。

爆發過濾器

通過GUI:

1. 登入到安全電子郵件網關的GUI。
2. 將滑鼠懸停在**安全服務**上。
3. 按一下**Outbreak Filters**。
4. 按一下**Edit Global Settings**。
5. 選中**Enable Outbreak Filters**。
6. 選中**Enable Web Interaction Tracking**。
7. 按一下「**Submit**」。
8. 按一下「**Commit**」。

通過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篩選

通過GUI:

1. 登入到安全電子郵件網關的GUI。
2. 將滑鼠懸停在**安全服務**上。
3. 按一下**URL Filtering**。
4. 按一下**編輯全域性設定。**
5. 選中**Enable URL Category and Reputation Filters**。
6. 選中**Enable Web Interaction Tracking**。
7. 按一下「**Submit**」。
8. 按一下「**Commit**」。

通過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互動追蹤

重要事實：

- 除非啟用Web互動跟蹤，否則不會填充報告模組。
- 報告不即時填充，它輪詢聚合器伺服器並每30分鐘獲取一次新資料。
- 可能需要2小時才能在跟蹤中看到點選事件。
- 報告可用於傳入和傳出郵件。
- 僅當策略或爆發過濾器重寫了URL時，才會報告URL按一下事件。

如果使用安全管理裝置(SMA)進行集中報告：

1. 登入到SMA。
2. 按一下**Email**頁籤。
3. 將滑鼠懸停在**Reporting**上。
4. 按一下**Web Interaction Tracking**。

雲端聯結器記錄

在較新版本的AsyncOS中，安全電子郵件網關現在支援Cloud Connector Logs，這是一個包含來自思科聚合伺服器的網路互動跟蹤的新日誌訂閱。新增該選項是為了在出現問題時幫助排除網路互動跟蹤故障。

通過GUI:

1. 登入到安全電子郵件網關GUI。
2. 將滑鼠懸停在**系統管理**上。
3. 按一下**Log Subscriptions**。

通過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
```

疑難排解

問題

無法連線到Cisco Aggregator Server。

解決方案

1. 從安全郵件網關ping Cisco Aggregator Server的主機名。您可以使用**aggregatorconfig**命令查詢主機名。
2. 驗證在**Security Services > Service Updates**中配置的代理連線。
3. 檢查防火牆、安全裝置和網路。

443 TCP 外寄 aggregator.cisco.com 訪問Cisco Aggregator伺服器。

- 從安全電子郵件網關Telnet至聚合器伺服器：telnet aggregator.cisco.com 443
- 從受影響的安全電子郵件網關對聚合器伺服器運行資料包捕獲。

4. 檢查DNS，確保伺服器的主機名在安全電子郵件網關上解析(在受影響的安全電子郵件網關上運行此命令：nslookup aggregator.cisco.com)。

問題

無法從Cisco Aggregator Server檢索Web互動跟蹤資訊。

解決方案

1. 驗證在**安全服務 > 服務更新**中配置的代理連線。
2. 檢查防火牆、安全裝置和網路。

443	TCP	外寄	aggregator.cisco.com	訪問Cisco Aggregator伺服器。

- 從安全電子郵件網關Telnet至聚合器伺服器：telnet aggregator.cisco.com 443
- 從受影響的安全電子郵件網關對聚合器伺服器運行資料包捕獲。

3. 檢查DNS，確保伺服器的主機名在裝置上解析(在受影響的安全電子郵件網關上運行此命令：nslookup aggregator.cisco.com)。

相關資訊

- 思科安全電子郵件網關最終使用手冊
- 思科安全電子郵件網關版本說明
- **技術支援與文件 - Cisco Systems**