什么是安全电邮中的思科聚合器服务器？

目录

简介

本文档介绍Cisco Aggregator Server是什么以及当安全邮件网关每30分钟轮询一次Cisco Aggregator Server（aggregator.cisco.com端口443）以获取Web交互跟踪数据时它如何工作。

什么是Cisco Aggregator Server，它如何工作？

安全邮件网关每30分钟轮询一次思科聚合器服务器（aggregator.cisco.com端口443），以获取Web交互跟踪数据。如果在爆发和过滤功能中启用，则Web交互跟踪报告显示以下数据：

- 点击的排名靠前的重写恶意URL。 点击恶意URL的人的列表。单击的时间戳。如果URL被策略或爆发过滤器重写。单击URL时，将采取操作：允许、阻止或未知。
- 点击重写的恶意URL的顶级人员。
- Web交互跟踪详细信息。 所有云重定向和重写的URL的列表。单击URL时，将采取操作：允许、阻止或未知。

注意：要显示Web交互详细信息，请确保选择**Incoming Mail Policies > Outbreak Filters** 以配置爆发过滤器并启用邮件修改和URL重写。使用重定向到思科安全代**理操作配置内容过**滤器。

配置思科聚合器服务器

```
> 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
```

如何启用Web交互跟踪

您可以通过两种不同的功能配置启用Web交互跟踪。

爆发过滤器

通过GUI:

1. 登录您的安全电子邮件网关的GUI。
2. 将鼠标悬停**在安全服务**上。
3. 单击“Outbreak Filters(**爆发过滤器**)”。
4. 单击“**编辑全局设置**”。
5. 选中**启用爆发过滤器**。
6. 选中**启用Web交互跟踪**。
7. 单击“Submit”。
8. 单击**Commit**。

通过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 过滤

通过GUI:

1. 登录您的安全电子邮件网关的GUI。
2. 将鼠标悬停**在安全服务**上。
3. 单击“**URL Filtering(URL过滤)**”。
4. 单击“**编辑全局设置”。**
5. 选中**启用URL类别和信誉过滤器。**
6. 选中**启用Web交互跟踪。**
7. 单击“Submit”。
8. 单击**Commit。**

通过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交互跟踪

重要事实：

- 除非启用Web交互跟踪，否则不会填充报告模块。
- 报告不实时填充，它轮询聚合器服务器并每30分钟获取一次新数据。
- 在跟踪中查看点击事件可能需要2小时。
- 报告可用于传入和传出邮件。
- 仅当URL被策略或爆发过滤器重写时，才会报告URL点击事件。

如果使用安全管理设备(SMA)进行集中报告：

1. 登录SMA。

2. 单击“Email(电**子邮件**)”选项卡。
3. 将鼠标悬停**在报告**上。
4. 单击“**Web Interaction Tracking**”。

云连接器日志记录

在AsyncOS的更新版本中，安全邮件网关现在支持云连接器日志，这是一个新的日志订用，包含来自思科聚合器服务器的Web交互跟踪。添加此项是为了在出现问题时帮助排除Web交互跟踪故障。

通过GUI:

1. 登录到您的安全邮件网关GUI。
2. 将鼠标悬停**在System Administration**上。
3. 单击**Log Subscriptions**。

通过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
```

故障排除

问题

无法连接到思科聚合器服务器。

解决方案

1. 从安全邮件网关对Cisco Aggregator服务器的主机名执行ping操作。您可以使用**aggregatorconfig**命令查找主机名。
2. 验证在“安全服务”>“服务更**新”中配置的代理连接**。
3. 检查防火墙、安全设备和网络。

443 TCP 输出 aggregator.cisco.com 访问思科聚合器服务器。

- 从安全邮件网关Telnet至聚合器服务器：telnet aggregator.cisco.com 443
- 从受影响的安全邮件网关向聚合器服务器运行数据包捕获。

4. 检查DNS，确保服务器的主机名在安全邮件网关上解析(在受影响的安全邮件网关上运行以下命令：nslookup aggregator.cisco.com)。

问题

无法从思科聚合器服务器检索Web交互跟踪信息。

解决方案

1. 验证在“安全服务”>“服务更**新”中配置的代理连接**。
2. 检查防火墙、安全设备和网络。

443 TCP 输出 aggregator.cisco.com 访问思科聚合器服务器。

- 从安全邮件网关Telnet至聚合器服务器：telnet aggregator.cisco.com 443
- 从受影响的安全邮件网关向聚合器服务器运行数据包捕获。

3. 检查DNS，确保服务器的主机名在设备上解析(在受影响的安全邮件网关上运行以下命令：nslookup aggregator.cisco.com)。

相关信息

- 思科安全电子邮件网关最终用户指南
- 思科安全电邮网关版本说明
- **技术支持和文档 - Cisco Systems**