如何在邮件安全设备和云邮件安全上存档邮件？

目录

简介

本文档介绍在邮件安全设备(ESA)和云邮件安全(CES)上存档邮件以进行检索和审核所需执行的步骤。

背景信息

当您在ESA和CES上存档电子邮件时，它可用于满足法规要求或为进一步的邮件诊断和审查提供额外的数据手段。存档电子邮件作为电子邮件的辅助存储，以邮箱日志格式（管理员的原始源）存储，以便检索和验证。

- 如果您决定启用电子邮件存档，建议将设置保留为默认值。默认值为每个日志10MB，最多保留10个日志。日志将继续根据日志文件本身的大小进行添加和滚动。存档邮箱日志文件根据通过设备的邮件流量的速率填充。创建更多日志后，旧的存档框日志将被删除，以释放空间来创建新日志。
- 在增加存档邮箱日志文件大小和保留的最大日志文件数之前，请确保您的设备有足够的磁盘空间。
- 为了停止生成存档邮箱日志，您必须按策略禁用存档功能。

注意：ESA和CES存档邮箱日志无法由安全管理设备(SMA)检索，并且在启用该功能的情况下按每个ESA和CES本地存储。

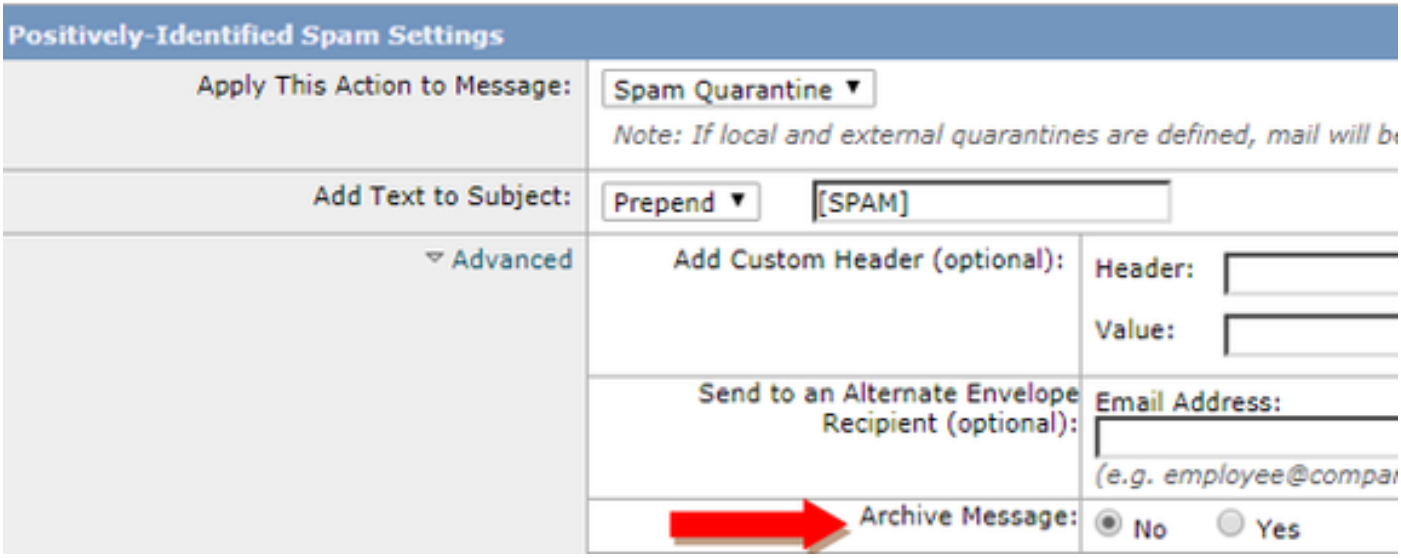
如何在ESA和CES上存档电子邮件？

邮件归档可通过反垃圾邮件、防病毒、高级恶意软件防护、灰色邮件和邮件过滤器提供。可通过图形用户界面(GUI)或命令行界面(CLI)为反垃圾邮件、防病毒、高级恶意软件防护和灰色邮件配置存档操作。

对于邮件过滤器，仅使用CLI即可配置存档操作。

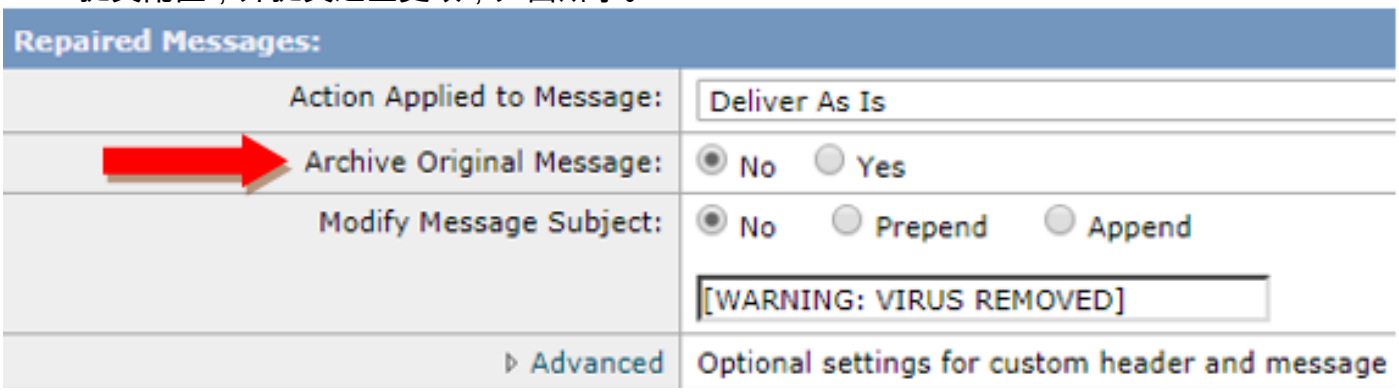
配置反垃圾邮件存档

1. 导航至GUI > Mail Policies > Incoming/Outgoing Mail Policies。
2. 单击相应策略的反垃圾邮件设置以配置电子邮件存档。
3. 点击“Advanced”（高级），查看“Proditial Identified Spam Settings”（确定的垃圾邮件设置）和/或“Suspected Spam”（可疑垃圾邮件）设置的可用设置。
4. 按“是”旁的单选按钮，以使用相应的反垃圾邮件判定来存档电子邮件。
5. 提交配置，并提交这些更改，如图所示。



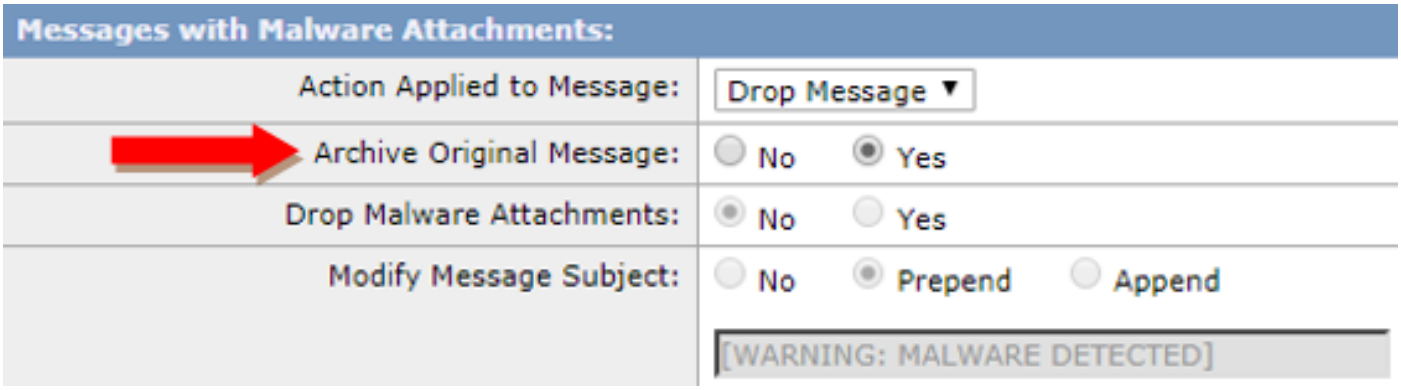
配置防病毒存档

1. 导航至GUI > Mail Policies > Incoming/Outgoing Mail Policies。
2. 单击相应策略上的防病毒设置以配置电子邮件存档。
3. 在要存档原始邮件的每个扫描判定上，按“是”旁边的单选按钮以存档。
4. 提交配置，并提交这些更改，如图所示。



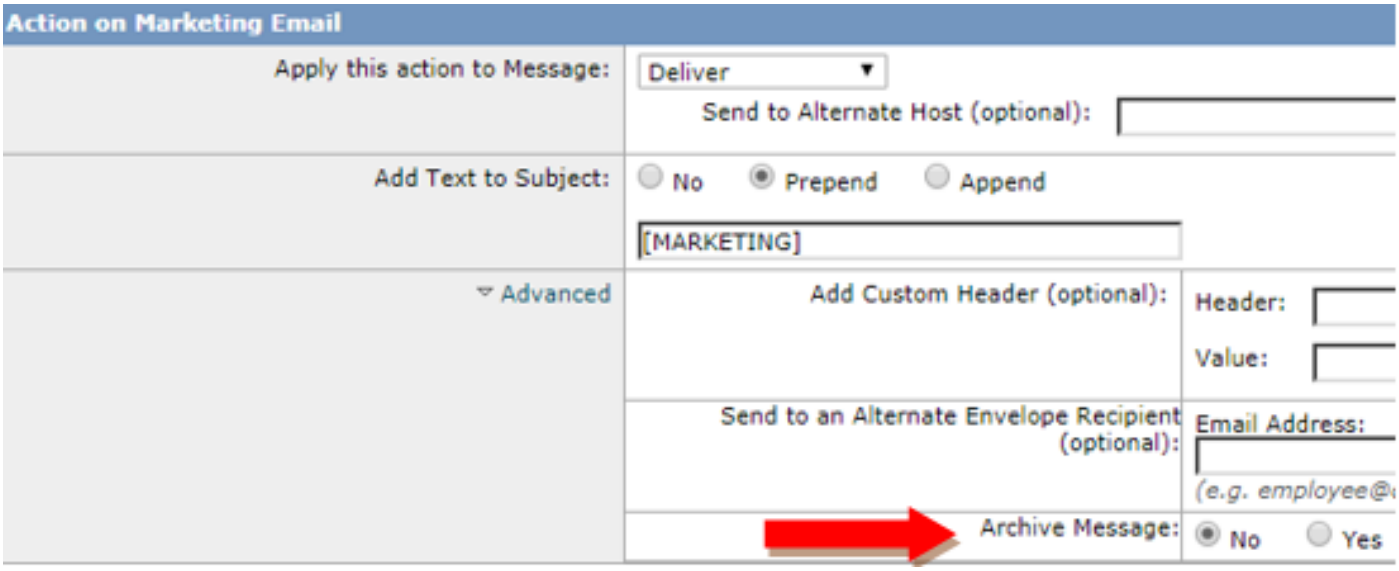
配置高级恶意软件防护存档

1. 导航至GUI > Mail Policies > Incoming/Outgoing Mail Policies。
2. 点击相应策略上的高级恶意软件防护设置以配置电子邮件存档。
3. 在要存档原始邮件的每个扫描判定上，按“是”旁的单选按钮以存档。
4. 提交配置，并提交这些更改，如图所示。



配置灰色邮件存档

1. 导航至GUI > Mail Policies > Incoming/Outgoing Mail Policies。
2. 单击相应策略上的灰色邮件设置以配置电子邮件存档。
3. 单击Advanced（高级），单击Marketing（营销）、Social（社交）、Bulk（批量）的可用设置。
4. 按“是”旁的单选按钮，以将电子邮件存档为相应的灰色邮件判定。
5. 提交配置并提交这些更改。



配置邮件过滤器存档

注意：要查看已存档日志，需要具有存档操作的邮件过滤器。邮件过滤器只能在CLI中创建。

过滤器示例：

```
Test_Archive:
if (mail-from == "test1@cisco.com")
{
archive("Test");
}
```

1. 登录CLI上的设备。
2. 创建消息过滤器，如提供的示例过滤器所示。
3. 提交此过滤器并提交更改。

验证存档邮箱日志可用性

当为各个服务提交存档配置时，存档的电子邮件以mbox格式日志文件存储。要验证归档日志是否可以检索，请导航至GUI > System Administration > Log Subscriptions。

安全服务归档创建具有归档日志类型的单独日志，如图所示：

Configured Log Subscriptions

Add Log Subscription...

Log Settings	Type ▲	Log Files	Rollover Interval
amp	AMP Engine Logs	amp/	None
amparchive	AMP Archive	amparchive/	None
antispam	Anti-Spam Logs	antispam/	None
antivirus	Anti-Virus Logs	antivirus/	None
asarchive	Anti-Spam Archive	asarchive/	None
authentication	Authentication Logs	authentication/	None
avarchive	Anti-Virus Archive	avarchive/	None

对于邮件过滤器，仅从CLI查看存**档配置**:

- **filters > logconfig**

```
demigod.cisco.com> filters

Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> logconfig

Currently configured logs:
    Log Name          Log Type                  Retrieval          Interval
 ----------------------------------------------------------------------------
 1. Test              Filter Archive Logs       Manual Download    None
```

检索Mbox日志

对于独立设备，这些mbox日志可以直接从GUI中检索。导航至**GUI > System Administration > Log Subscription，然**后单击要检索**的相**应存档日志的Log Files。

对于集群设备，可使用FTP/安全复制(SCP)来检索mbox日志，如本文所[述](https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118315-technote-esa-00..)。(https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118315-technote-esa-00..。 .)

相关信息

- 思科邮件安全设备 — 最终用户指南
- UNIX邮箱格式是什么？
- 思科邮件安全设备(ESA)上存储的日志的位置以及如何访问这些日志
- 如何从存档邮箱日志中提取电子邮件
- 技术支持和文档 - Cisco Systems