如何归档在电子邮件安全工具和Cloud上的电子邮件给安全发电子邮件？

Contents

Introduction

本文描述将被跟随的步骤为了归档在电子邮件安全工具(ESA)和Cloud电子邮件安全(CES)上的电子邮件检索和复核的。

背景信息

当您归档在ESA和CES时的电子邮件，可以用于符合章程要求或为进一步邮件诊断和复核提供数据另外的平均值。归档发电子邮件作为电子邮件的间接储藏以在它的mbox日志格式是管理员的初始源为了检索和验证。

- 如果决定对enable (event)归档电子邮件，推荐保持设置到默认值。默认值是10MB每个保留的日志和10本日志最大数量。日志将继续被添加和滚动基于日志文件的大小。档案mbox日志文件被填装根据虽则通过工具的电子邮件数据流的费率。当更多日志被创建，更旧的档案mbox日志被去除对新的日志的创建的空闲空间。
- 保证您的设备有充足的磁盘空间，在您增加保留前的档案mbox日志文件大小和最大日志文件。
- 为了从生成终止档案mbox日志，您将必须禁用档案功能每个策略。

Note:ESA和CES档案mbox日志不可能由SMA检索和每个每个ESA和CES存储本地有功能功能。

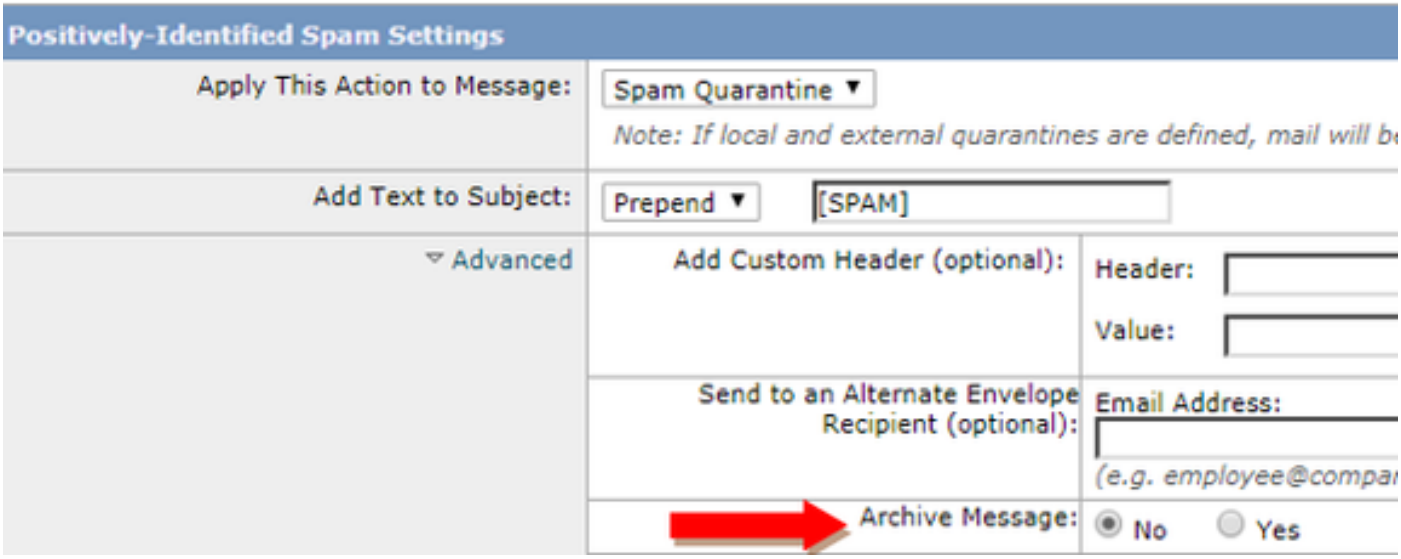
如何归档在ESA和CES的电子邮件？

电子邮件归档用反垃圾邮件，抗病毒，先进的Malware保护、Graymail和消息过滤器是可用的。 档案动作可以在GUI和CLI被配置反垃圾邮件、抗病毒，先进的Malware保护和Graymail的。

档案动作可以在仅CLI被配置消息过滤器的。

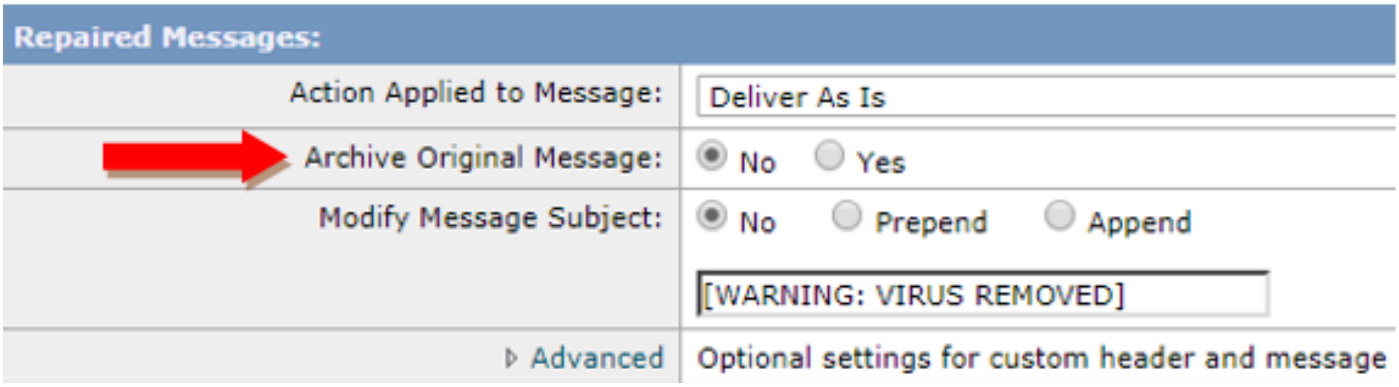
配置反垃圾邮件档案

1. 连接对**GUI >邮件策略>流入/流出的邮件策略。**
2. 点击在各自策略的反垃圾邮件设置为了配置电子邮件归档。
3. 点击**先进**在确实地被识别的垃圾邮件设置的可用的设置，怀疑的垃圾邮件设置。
4. 在是旁边按单选按钮为了归档与各自反垃圾邮件判决的电子邮件。
5. 如镜像所显示， Submitthe配置，和确认这些更改。



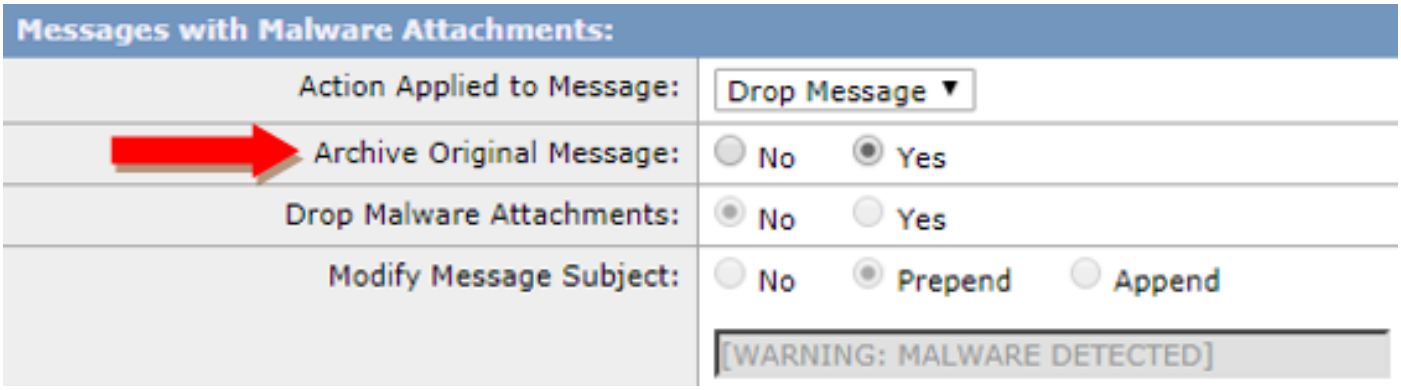
配置抗病毒档案

1. 连接对**GUI >邮件策略>流入/流出的邮件策略。**
2. 点击在各自策略的抗病毒设置为了配置电子邮件归档。
3. 在其中每一扫描您希望归档原始消息的判决，在是旁边按单选按钮在orderto档案里。
4. 如镜像所显示， Submitthe配置，和确认这些更改。



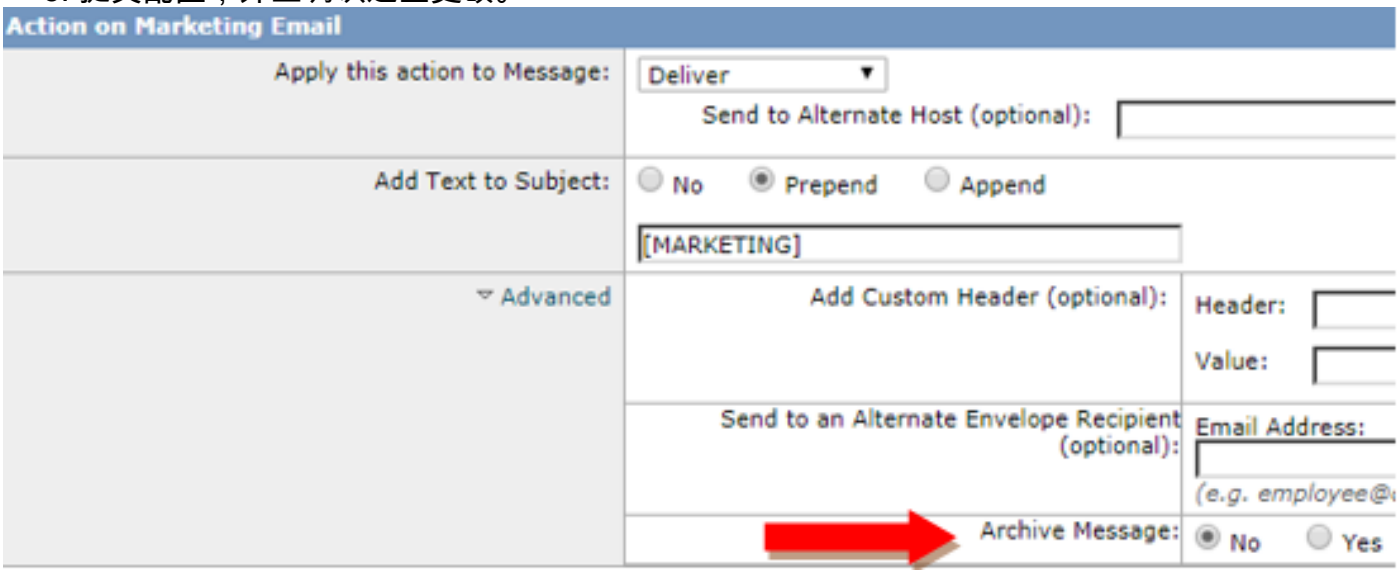
配置先进的Malware保护档案

1. 连接对**GUI >邮件策略>流入/流出的邮件策略。**
2. 点击在各自策略的先进的Malware Protectionsettings为了配置电子邮件归档。
3. 在其中每一扫描您希望为了归档原始消息的判决，在是旁边按单选按钮为了归档。
4. 如镜像所显示， Submitthe配置，和确认这些更改。



配置Graymail档案

1. 连接对**GUI >邮件策略>流入/流出的邮件策略。**
2. 点击在各自策略的Graymail设置为了配置电子邮件归档。
3. 点击**Advancedon**销售的可用的设置，社交，容量。
4. 在是旁边按单选按钮为了归档与各自Graymail判决的电子邮件。
5. 提交配置，并且确认这些更改。



配置消息过滤器档案

> **Note**: 要求有档案动作的一台消息过滤器为了查看归档日志。消息过滤器可能在CLI内只被创建。

示例过滤器：

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

1. 设备的洛金在CLI。
2. 如在提供的示例过滤器中看到创建一台消息过滤器。
3. 提交此过滤器并且确认您的更改。

验证档案Mbox日志可用性

当档案的配置为各自服务时被提交，归档的电子邮件在mbox格式日志文件存储。为了验证归档日志是否为检索是可用的，请连接对**GUI >System Administration >日志订阅**。

如镜像所显示，安全服务档案用归档日志类型创建一本单独的日志：

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

对于消息过滤档案配置从**CLI只查看**：

- **过滤器> 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日志可以直接地从GUI被检索。连接对theGUI **>System Administration >日志Subscriptionsand**点击您将检索的各自归档日志的**日志文件**。

对于集群的工具， mbox日志可以检索与使用FTP/Secure复制(SCP)正如**thisarticle所描述**。(https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118315-technote-esa-00....)

Related Information

- Cisco电子邮件安全工具-终端用户指南
- 什么是UNIX mbox (邮箱)格式？
- 那里在Cisco电子邮件安全工具存储的日志(ESA)，并且I如何访问他们
- 如何从档案mbox日志提取电子邮件
- Technical Support & Documentation - Cisco Systems