配置邮件安全设备以允许模拟网络钓鱼活动

目录

[简介](#)

[先决条件](#)

- [要求](#)
- [使用的组件](#)

[背景信息](#)

[原因](#)

[解决方案](#)

- [AsyncOS 13.x及更低版本](#)

简介

本文档介绍如何配置邮件安全设备(ESA)以允许模拟网络钓鱼平台活动成功通过。

先决条件

要求

Cisco 建议您了解以下主题：

- 在思科邮件安全设备(ESA)上创建邮件和内容过滤器。
- 主机访问表(HAT)的配置。
- 了解Cisco ESA传入邮件管道。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

通过模拟网络钓鱼平台，管理员可以运行网络钓鱼活动以进行安全感知测试。

原因

当思科ESA未配置为信任模拟网络钓鱼平台主机时，安全扫描和策略控制可以阻止活动邮件。此行为可能会导致活动失败或降低模拟的有效性。

解决方案

⚠ 警告：在此配置示例中，选择TRUSTED邮件流策略，以允许思科ESA通过更大的模拟网络钓鱼活动，而不会有任何限制。持续进行大量网络钓鱼活动可能会影响邮件处理性能。

为了确保思科ESA不会停止活动消息，请配置专用发件人组并绕过平台主机的扫描。

1.定位至GUI >邮件策略> HAT概述。

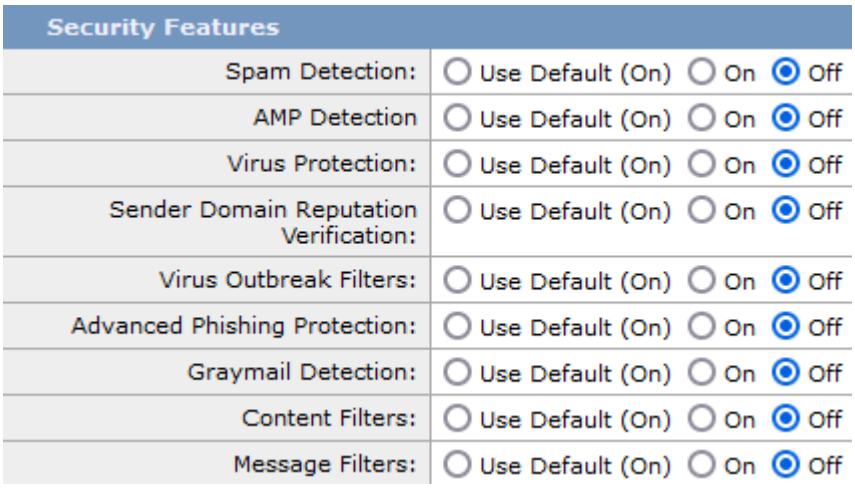
2.创建新的发件人组，并将其绑定到TRUSTED邮件流策略。或者，在GUI > Mail Policies > Mail Flow Policies下使用类似的选项创建新策略。

3.将模拟网络钓鱼平台的发送主机或IP地址添加到此发件人组。如果模拟网络钓鱼平台使用大型IP地址范围，请添加部分主机名或IP范围（如果适用）。

4.对BLOCKLIST发件人组之前的发件人组进行排序，以确保静态匹配该组，而不是SBRS。

5.定位至GUI >“邮件策略”>“邮件流策略”>“受信任”，或定位至新创建的邮件流策略。

6.禁用该受信任策略的所有安全功能，如屏幕截图所示。



6.提交更改并提交配置。

AsyncOS 13.x及更低版本

⚠ 警告：在此配置示例中，选择TRUSTED邮件流策略，以允许思科ESA通过更大的模拟网络钓鱼活动，而不会有任何限制。持续进行大量网络钓鱼活动可能会影响邮件处理性能。

要确保网络钓鱼活动消息不会被思科ESA的任何安全组件拦截，需要实施配置。

1.定位至GUI >邮件策略> HAT概述。

2.创建新的发件人组，并将其绑定到TRUSTED邮件流策略。

3.将模拟网络钓鱼平台的发送主机或IP添加到此发件人组。如果模拟网络钓鱼平台具有大范围的IP，您可以添加部分主机名或IP范围（如果适用）。

4.对BLOCKLIST Sender组之前的发件人组进行排序，以确保静态匹配该组，而不是BS。

5.提交并提交这些更改，

6.导航到命令行界面(CLI)。

7.运行过滤器。

8.创建新的邮件过滤器。复制语法，针对环境对其进行修改，然后添加过滤器。

```
skip_engines_for_simulated_phishing:
if (sendergroup == "name_of_the_newly_created_sender_group")
{
insert-header("x-sp", "uniquevalue");
log-entry("Skipped scanning engines for simulated phishing");
skip-spamcheck();
skip-viruscheck();
skip-ampcheck();
skip-marketingcheck();
skip-socialcheck();
skip-bulkcheck();
skip-vofcheck();
skip-filters();
}
.
```

9.将列表中的邮件过滤器向上排序，以确保其他邮件过滤器（包括跳过过滤器操作）不会跳过该邮件过滤器。

10.按Enter返回主AsyncOS命令提示符。

11.运行commit以保存更改。

12.不要按Ctrl+C。它会清除更改。

13.导航到GUI >“邮件策略”>“传入内容过滤器”。

14.创建新的传入内容过滤器。

15.将条件设置为Other Header。

16.配置过滤器以查找自定义报头x-sp以及在邮件过滤器中配置的唯一值。

17. 将操作设置为Skip Remaining Content Filters(Final Action)。

18.将内容过滤器排序为1，以确保其他过滤器不对模拟网络钓鱼邮件采取行动。

19.导航到GUI > Mail Policies > Incoming Mail Policies。

20.将内容过滤器分配给所需的策略。

21.提交并提交更改。

22.开展模拟网络钓鱼平台活动。

23.监控mail_logs或邮件跟踪，以验证邮件流和策略规则匹配。

24.预期成果：思科ESA接受活动消息，匹配配置的发件人组和过滤器，并绕过为受信任策略配置的扫描操作。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。