创建在Cisco ESA的一项Whitelist策略网络钓鱼教育测验的

目录

[简介](#)
[先决条件](#)
[要求](#)
[背景信息](#)
[配置](#)
[创建发送方组](#)
[创建消息过滤器](#)
[验证](#)

简介

本文描述如何创建在Cisco电子邮件安全工具(ESA)或Cloud电子邮件安全(CES)实例的一项Whitelist策略允许网络钓鱼教育测验/市场活动。

先决条件

要求

Cisco 建议您了解以下主题：

- 导航和配置在Cisco ESA/CES的规则在WebUI。
- 创建在Cisco ESA/CES的消息过滤器在命令行界面(CLI)。
- 用于网络钓鱼活动的资源的知识/测验。

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

执行网络钓鱼教育测验或市场活动的管理员把电子邮件生成与将匹配在反垃圾邮件和爆发过滤规则集的当前Talos规则的信息。在这样事件，网络钓鱼活动电子邮件不会到达最终用户和由因而导致测验的Cisco ESA/CES actioned止步不前。管理员会需要保证ESA/CES通过这些电子邮件允许执行他们的活动/测验。

配置

> 警告：在whitelisting的网络钓鱼仿真&教育供应商的Cisco的姿态全局没有允许。我们建议管理员工作与网络钓鱼模拟程序服务*(例如：)*获取他们的IP的*PhishMe*然后添加他们本地到Whitelist。如果他们转换所有权或实际上变为威胁， Cisco必须保护我们的从那些IP的

ESA/CES客户。

警告：管理员在Whitelist应该只保留这些IP，当测试时，留下在Whitelist的外部IP长时间请张贴测试可以给最终用户带来未经请求的或有恶意的电子邮件如果被变得的这些IP折衷。

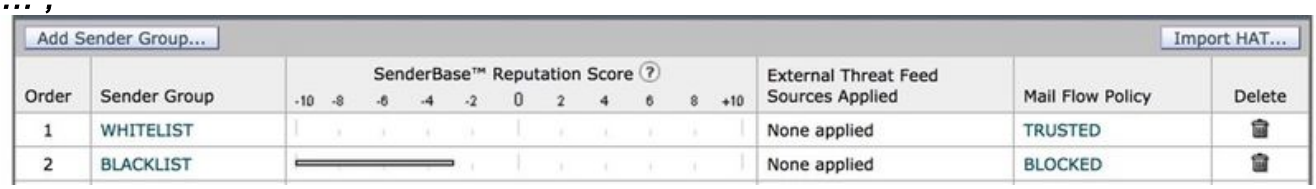
在Cisco电子邮件安全工具(ESA)上，请创建您的网络钓鱼仿真的一新的发送方组并且分配它到$TRUSTED邮件流量策略。这将允许将传送的所有网络钓鱼仿真电子邮件对最终用户。此的成员新建的发送方组不是受限制的速率支配，并且从那些发送方的内容没有乘Cisco IronPort反垃圾邮件引擎扫描，然而由防病毒软件仍然扫描。

Note:默认情况下， $TRUSTED邮件流量策略有被关闭的防病毒启用的，但是反垃圾邮件。

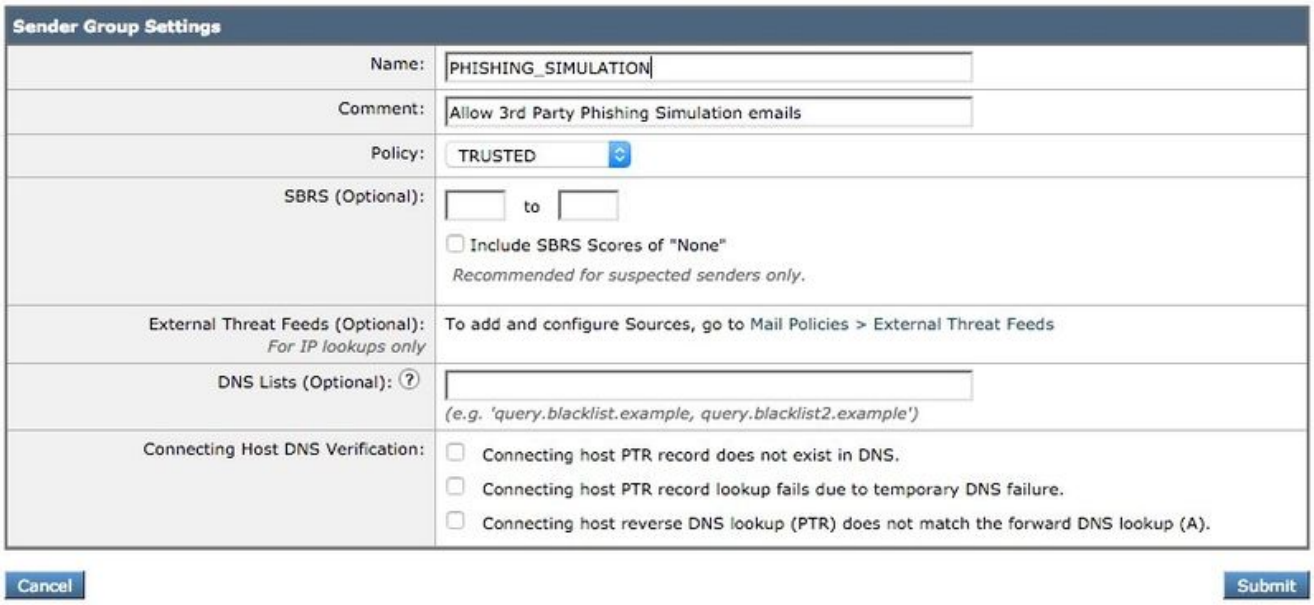
创建发送方组

1. 点击***邮件Policies选项***。
2. 在***主机访问表***部分下，请选择***帽子概述***

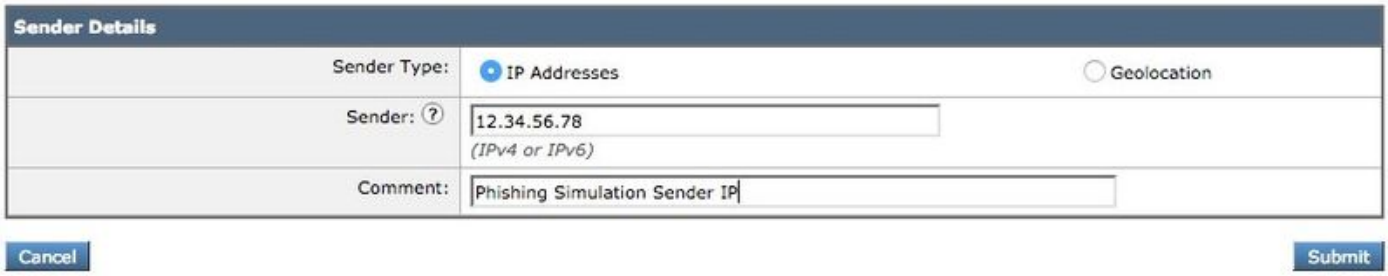
3. 在右边，请确保您的*InboundMail*监听程序当前选择，
4. 从下面***发送方组的***列，请单击***添加发送方组…***，



5. 填写***名称***和***注解栏***。 根据下拉式的***策略***，请选择"**$TRUSTED**'然后单击***提交并且添加发送方>>。***



6. 输入您希望对Whitelist在第一个字段的IP或主机名。 您的网络钓鱼仿真合作伙伴将提供您发送方IP信息。



当您完成添加条目时，请点击***SUBMIT按钮***。切记点击***进行更改***按钮保存您的更改。

创建消息过滤器

在创建发送方组以后允许反垃圾邮件和防病毒旁路，消息过滤器要求跳过可能匹配网络钓鱼活动/测验的其他安全引擎。

1. 对ESA的CLI的连接。
2. 运行命令***过滤器***。
3. 运行new命令创建一个新的消息过滤器。
4. 若需要复制和插入以下过滤器示例，进行为您的实际发送方组名编辑：

```
skip_amp_graymail_vof_for_phishing_campaigns:
if(sendergroup == "PHISHING_SIMULATION")
{
skip-ampcheck();
skip-marketingcheck();
skip-socialcheck();
skip-bulkcheck();
skip-vofcheck();
}
```

5. 返回到主CLI提示符并且按回车。
6. 运行***进行***保存配置。

验证

请使用第三方资源发送网络钓鱼活动/测验，并且验证在消息跟踪日志的结果保证所有引擎被跳过了，并且电子邮件传送。