排除ESA上的常见HAT/RAT错误

目录

简介

概述

- HAT
- 发件人组
- SenderBase信誉得分
- 应用外部威胁源(ETF)源
- 邮件流策略
- RAT

常见实施方案

- 手动阻止发件人
- 将IP地址组/范围添加到HAT中

故障排除

- 发件人匹配不正确的发件人组
- 发件人组主机配置不正确
- HAT/RAT拒绝是否计入“由信誉过滤拦截”？
- 通过RAT表检验拒绝
- 如何记录被拒绝连接的其他发件人/收件人信息？

相关信息

简介

本文档介绍用于诊断邮件安全设备(ESA)上的主机访问表(HAT)和收件人访问表(RAT)常见问题的高级概述、配置指南和故障排除技术。

概述

HAT

对于每个已配置的侦听程序，必须定义一组规则来控制来自远程主机的传入连接。例如，您可以定义远程主机以及它们是否可以连接到侦听程序。AsyncOS允许您定义允许哪些主机使用HAT连接到侦听程序。

HAT维护一组规则，这些规则控制来自侦听程序的远程主机的传入连接。每个已配置的监听程序都有其自己的独立HAT。可以为公共侦听程序和专用侦听程序配置HAT。

默认情况下，HAT被定义为根据侦听程序类型采取不同的操作：

- 公共侦听程序：HAT设置为接受来自所有主机的电子邮件。
- 专用侦听程序：HAT配置为中继来自指定主机的邮件，并拒绝所有其他主机。

HAT规则包括发件人组、SenderBase信誉得分(SBRS)、应用的外部威胁源以及邮件流策略。

发件人组

发件人组是由以下一个或多个标识的发件人列表：

- IP地址（IPv4或IPv6）
- IP 范围
- 特定主机或域名
- IP信誉服务“组织”分类
- IP信誉得分(IPRS)范围（或缺少得分）
- DNS列表查询响应

SenderBase信誉得分

设备可以查询IP信誉服务以确定IP信誉得分。IP信誉得分是根据IP信誉服务信息分配给IP地址、域或组织的数字值。

应用外部威胁源(ETF)源

ETF框架允许ESA使用通过TAXII协议传输的STIX格式外部威胁信息。

能够使用外部威胁信息，可帮助组织：

- 主动应对网络威胁，如恶意软件、勒索软件、网络钓鱼攻击和针对性攻击。
- 订阅本地和第三方威胁情报源。
- 提高功效。

您需要有效的功能密钥才能在ESA上使用ETF。有关如何获取功能密钥的信息，请联系您的思科销售代表和/或思科全球许可运营。

邮件流策略

邮件流策略允许您控制或限制在SMTP会话期间从发件人到侦听程序的电子邮件流。可以通过在邮件流策略中定义以下类型的参数来控制SMTP会话：

- 连接参数（例如，每个连接的最大消息数）
- 速率限制参数（例如，每小时的最大收件人数）
- 自定义SMTP代码和响应在SMTP会话期间进行通信
- 启用/禁用反垃圾邮件检测
- 启用/禁用防病毒保护
- 加密（例如，TLS）
- 身份验证和验证（例如，DMARC、DKIM和SPF）

RAT

AsyncOS对每个公共侦听程序使用RAT来管理收件人地址的接受或拒绝。收件人地址包括：

- 域
- 邮件地址
- 电子邮件地址组

默认情况下，RAT拒绝所有收件人，以阻止创建开放中继。

常见实施方案

手动阻止发件人

要按发件人IP地址阻止特定发件人，请在阻止列表发件人组下为IP地址添加手动条目，并确保将操作设置为“拒绝”或“TCP拒绝”。 有关配置说明，请参阅在ESA上手动阻止发件人IP。

将IP地址组/范围添加到HAT中

相邻IP地址可以划分为子网(例如192.0.2.0/24)、IP地址范围（例如192.0.2.10-20）或部分IP地址（例如192.0.2.）并添加到表中。要添加多个非相邻IP地址，请遵循以下步骤：

从 GUI：

1. 导航到邮件策略> HAT概述（如有必要，选择相应的集群级别）。
2. 选择Sender Group进行修改，然后选择Add Sender。
3. 在Sender字段中，输入适用的IP范围(例如，192.0.2.0/24)以及可选注释，然后选择Submit。
4. 单击Commit Changes保存。

从 CLI：

1. 运行命令序列：

   <#root>

   listenerconfig >> EDIT

2. 输入要编辑的监听程序的名称或编号。
3. 运行命令序列，然后输入要编辑的发件人组编号或名称：

   HOSTACCESS >> EDIT >> 1

4. 选择new并输入要添加的以逗号分隔的发件人列表。
5. 完成后，运行commit以保存更改。

故障排除

发件人匹配不正确的发件人组

验证ESA上的邮件日志或安全管理设备(SMA)上的邮件跟踪，并检查传入连接ID(ICID)中的以下条目：

```
ICID 476946 ACCEPT SG WhiteList match nx.example SBRS None country United States
```

理由：已在发件人组上启用连接主机DNS验证，并且已选择在DNS中不存在连接主机PTR记录。

```
ICID 476946 ACCEPT SG WhiteList match not.double.verified.example SBRS None country United States
```

理由：已在发件人组上启用连接主机DNS验证，并且已选择连接主机反向DNS查找(PTR)与正向DNS查找(A)不匹配。

```
ICID 476946 ACCEPT SG WhiteList match serv.fail.example SBRS None country United States
```

理由：已在发件人组上启用连接主机DNS验证，并且由于选择临时DNS故障，连接主机PTR记录查找失败。

发件人组主机配置不正确

发件人组是由以下内容标识的发件人列表：

- IP地址（IPv4或IPv6）
- IP 范围
- 特定主机或域名
- IP信誉服务“组织”分类
- IP信誉得分(IPRS)范围（或缺少得分）
- DNS列表查询响应

发件人组下配置错误的地址示例：ESA发件人组匹配部分主机名。

HAT/RAT拒绝是否计入“由信誉过滤拦截”？

是，发件人组拒绝且邮件流策略中执行拒绝操作的邮件将计入“由信誉过滤拦截”(Stopped by Reputation Filtering)报告计数器中。

注意：此计数器可以包括HAT策略拒绝和基于SBRS的拒绝。验证邮件日志中的拒绝原因以区分来源。

通过RAT表检验拒绝

以下是ESA上邮件日志的日志输出示例：

```
Thu Sep 18 09:10:14 2014 Info: MID 48445 ICID 15970 To: <user@example.com> "Rejected by RAT"
```

理由：ESA配置中的RAT下不允许特定域。

如何记录被拒绝连接的其他发件人/收件人信息？

默认情况下，拒绝的连接仅将发件人MTA IP地址记录在邮件日志中，而不记录信封发件人或信封收件人。如果故障排除需要其他日志记录，则可以在AsyncOS上启用延迟的HAT拒绝。

⚠ 警告：Cisco建议您不要永久启用此功能，因为它需要额外的资源。

有关详细信息，请参阅：HAT延迟拒绝常见问题

相关信息

- 思科邮件安全设备 — 最终用户指南
- 思科技术支持和下载

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）。