IP 信誉过滤

本章包含以下部分：

- 发件人 IP 信誉过滤概述, on page 1
- IP 信誉服务, on page 1
- 编辑侦听程序的 IP 信誉过滤得分阈值 , on page 4
- 在邮件主题中输入低 IP 信誉得分, on page 6

发件人 IP 信誉过滤概述

发件人 IP 信誉过滤是垃圾邮件的第一道防线，允许您基于 发件人 IP 信誉服务确定的发件人信誉来控制通过邮件网关的邮件。

邮件网关可以接受来自已知或高信誉发件人（例如客户和合作伙伴）的邮件，并直接将它们传送给最终用户，不进行任何内容扫描。来自未知或低信誉发件人的邮件可能需要接受内容扫描，例如反垃圾邮件和防病毒扫描，也可以限制您愿意从每个发件人那里接受的邮件数。对于信誉最差的邮件发件人，可以根据首选项设置拒绝其连接或退回邮件。

Note 文件信誉过滤是一项独立服务。有关信息，请参阅文件信誉过滤和文件分析：

IP 信誉服务

IP 信誉服务使用 Talos 成员网络中的全球数据，基于抱怨次数、邮件数量统计数据及公共阻止列表和开放式代理列表中的数据，向邮件发件人分配一个 IP 信誉得分 (IPRS)。IP 信誉得分有助于区分合法发件人与垃圾邮件来源。您可以决定阻止信誉得分低的发件人的邮件数量阈值。

Talos 安全网络网站 (https://talosintelligence.com) 提供最新邮件和网络威胁的全局概述，按国家/地区显示当前的邮件流量，并允许您根据 IP 地址、URL 或域查询信誉得分。

相关主题

- IP 信誉得分 , on page 2

- Sender IP 信誉过滤器工作原理 , on page 3
- 不同发件人 IP 信誉过滤方法的建议设置 , on page 3
- 病毒爆发过滤器
- 使用邮件安全监控

IP 信誉得分

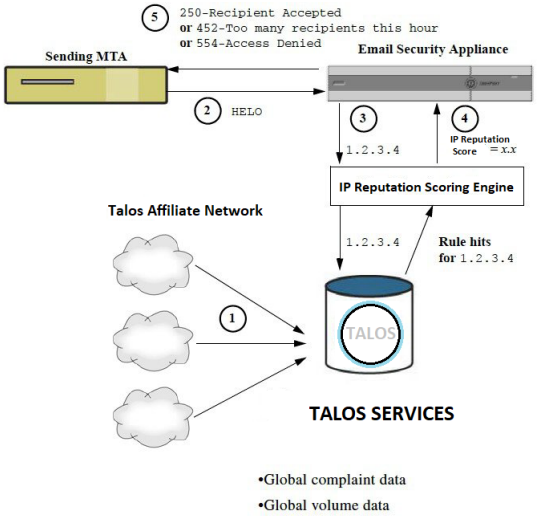
IP 信誉得分 是基于 IP 信誉服务中的信息分配给 IP 地址的数值。IP 信誉服务整合 25 个公共阻止列表和开放式代理列表中的数据，并将此数据与 Talos 中的全球数据合并，进而分配一个介于 -10.0 到 +10.0 之间的分数，如下所示：

得分	含义
-10.0	很可能是垃圾邮件的来源
0	中立；或信息不足，无法提供相关建议
+10.0	很可能是可信发件人

得分越低（负值越大），越有可能是垃圾邮件。得分为 -10.0，表示此邮件“一定”是垃圾邮件；而得分为 10.0，表示邮件“一定”是合法的。

使用 IP 信誉得分，可以将邮件网关配置为基于发件人的可信度对发件人应用邮件流策略。（还可以创建邮件过滤器来指定 IP 信誉得分的“阈值”，进一步对系统处理的邮件执行操作。有关详细信息，请参阅IP 信誉规则和绕过反垃圾邮件系统操作。）

***Figure 1: IP* 信誉服务**



1. Talos 成员实时发送全球数据
2. 发送 MTA 将打开与邮件网关的连接
3. 邮件网关检查连接 IP 地址的全球数据
4. IP 信誉服务计算此邮件是垃圾邮件的概率，并分配 IP 信誉得分

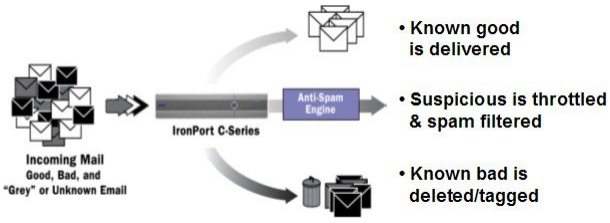
5. 思科根据 IP 信誉得分返回响应

Sender IP 信誉过滤器工作原理

发件人 IP 信誉过滤器技术旨在从邮件网关中可用的剩余安全服务处理中，转轨尽可能多的邮件。（请参阅了解邮件通道。）

启用发件人信誉过滤时，将简单拒绝已知恶意发件人的邮件。来自全球2000家公司的已知正常邮件会自动路由到垃圾邮件过滤器，降低误报的可能性。未知或“灰色”邮件将路由到反垃圾邮件扫描引擎。使用此方法，发件人 IP 信誉过滤器可使内容过滤器的负载降低多达 50%。

Figure 2: 发件人 ***IP*** 信誉过滤示例



不同发件人 IP 信誉过滤方法的建议设置

根据企业目标，可以实施保守、中等或主动方法。

方案	特征	Allowed _List	Blocked_ List	可疑列表	未知列表
		发件人 IP 信誉得分范围：			
保守	接近零误报，较好性能	7 到 10	-10 到 -4	-4 到 -2	-2 到 7
中等 （系统设定值）	很少误报，高性能	不使用发件人 IP 信誉得分。	-10 到 -3	-3 到 -1	-1 到 +10
积极	有些误报，最高性能。 此选项将从反垃圾邮件处理中转轨大多数邮件。	4 到 10	-10 到 -2	-2 到 -1	-1 到 4
所有方法		**邮件流策略：**			
		可信	阻止	受限	已接受

编辑侦听程序的 IP 信誉过滤得分阈值

如果要更改默认 IP 信誉服务 得分阈值或添加信誉过滤的发件人组，请使用此步骤。

Note 使用主机访问表定义允许连接的主机中介绍了有关 IP 信誉得分阈值的其他设置及邮件流策略设置。

准备工作

- 如果您的邮件网关设置为从本地 MX/MTA 接收邮件，请标识出可能会屏蔽发件人 IP 地址的上游主机。有关详细信息，请参阅通过传入中继确定部署中的发件人 IP 地址。
- 了解 IP 信誉得分。请参阅按 IP 信誉得分定义发件人组。
- 选择适合您的组织的过滤方法，并注意针对该方法的建议设置。请参阅不同发件人 IP 信誉过滤方法的建议设置 , on page 3。

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **HAT 概述 (HAT Overview)**。

步骤 2 从**发件人组(监听程序) (Sender Groups (Listener))** 菜单中选择公共监听程序。

步骤 3 单击某个发件人组的链接。

例如，单击“SUSPECTLIST”链接。

步骤 4 单击**编辑设置 (Edit Settings)**。

步骤 5 针对此发件人组，输入 IP 信誉得分范围。

例如，对于“ALLOWED_LIST”，输入范围 7.0 到 10。

步骤 6 单击**提交 (Submit)**。

步骤 7 根据需要，针对此监听程序的每个发件人组重复上述操作。

步骤 8 确认更改。

What to do next

相关主题

- 使用 IP 信誉得分测试 IP 信誉过滤, on page 5
- 使用主机访问表定义允许连接的主机
- 如何配置邮件网关以扫描垃圾邮件

使用 IP 信誉得分测试 IP 信誉过滤

除非定期接收大部分垃圾邮件或已设置“虚拟”帐户来专门接收组织的垃圾邮件，否则可能很难立即测试实施的 IP 信誉策略。但是，如果您将使用 IP 信誉得分的信誉过滤条目添加到了下表中所示的监听程序 HAT 中，会看到有小比例的传入邮件为“未分类”。

使用任意 IP 信誉得分 的 `trace` 命令来测试策略。请参阅使用测试邮件调试邮件流：追踪。在 CLI 和 GUI 中都可使用 `trace` 命令。

Table 1: 实施 ***IP*** 信誉得分的建议邮件流量策略

策略名称	主要行为（访问规则）	参数	值
`$BLOCKED`	`REJECT`	`None`	
`$THROTTLED`	`ACCEPT`	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: Use Spam Detection: Use TLS: Maximum recipients / hour: Use SenderBase:	10 20 1 MB 10 ON OFF **20**（建议） 开启
`$ACCEPTED` （公共监听程序）	`ACCEPT`	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: Use Spam Detection: Use TLS: Use SenderBase:	1,000 1,000 100 MB 1,000 ON OFF 开启
`$TRUSTED`	`ACCEPT`	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: Use Spam Detection: Use TLS: Maximum recipients / hour: Use SenderBase:	1,000 1,000 100 MB 1,000 关闭 关闭 -1 （已禁用） 关闭

Note 在 $THROTTLED 策略中，每小时来自远程主机的最大收件人数默认设置为每小时 20 位收件人。请注意，此设置控制最大可用限制。如果此参数过于严格，可以提高每小时接收的收件人数。有关默认主机访问策略的详细信息，请参阅了解预定义发件人组和邮件流策略。

在邮件主题中输入低 IP 信誉得分

虽然思科建议执行限制，不过使用 IP 信誉服务的另一种方法是修改可疑垃圾邮件的主题行。为此，请使用下表中所示的邮件过滤器。此过滤器使用 reputation 过滤器规则以及 strip-header 和 insert-header 过滤器操作，将 IP 信誉得分低于 -2.0 的邮件主题行替换为包括实际 IP 信誉得分的主题行，表示形式为：**{Spam** *IP Reputation Score***}**。在本例中，会将 *listener_name* 替换为您的公共监听程序。（包括其自有行中的句号，以便可以直接剪切此文本并粘贴到 filters 命令的命令行界面。）

表：使用 IP 信誉修改主题信头的邮件过滤器：示例 1

```
iprs_filter:

if ((recv-inj == "listener_name
" AND subject != "\\{Spam -?[0-9.]+\\}"))

{

        insert-header("X-IPRS", "$REPUTATION");

        if (reputation <= -2.0)

{

        strip-header("Subject");

        insert-header("Subject", "$Subject \\{Spam $REPUTATION\\}");

       }

 }

.
```

相关主题

- 使用邮件过滤器实施邮件策略