发件人域信誉过滤

本章包含以下部分：

发件人域信誉过滤概述

思科 Talos 发件人域信誉（SDR）是一种云服务，可根据邮件信封和标题中提供的域名为邮件提供信誉判定。示例可能包括域：HELO/EHLO 字符串、信封和信头“From”地址、“Reply-to”地址和“List-Unsubscribe”信头。

基于域的信誉分析通过查看共享 IP 地址、托管或基础设施提供程序的信誉，并根据与完全限定域名 (FQDN) 相关的功能以及简单邮件传输协议 (SMTP) 对话和邮件信头中的其他发件人信息衍生判定，从而实现更高的垃圾邮件捕获率。

从 AsyncOS 14.2.x 版本开始，发件人域有效期选项将替换为发件人成熟度。发件人成熟度是建立发件人信誉的重要功能。发件人成熟度是根据多个信息源自动生成的，用于垃圾邮件分类，可能不同于“基于 Whois 的域期间。” 发件人成熟度被设为 30 天限制，如果超过该限制，域就会被视为邮件发件人的成熟地址，并且不会提供进一步的详细信息。

从此版本开始，在收到邮件的发件人信头后，将执行额外的发件人域信誉检查。威胁级别与配置的 SDR 拒绝级别（在您的邮件网关中）匹配的邮件将被拒绝。

注释 从此版本开始，“SDR 域期限”配置的过滤器将自动更新为“SDR 发件人成熟度”过滤器。升级后，发件人成熟度值无效的过滤器将被标记为“非活动”。确保相应地查看和修改消息和内容过滤器。

注释 发件人成熟度功能使用邮件网关的当前时间在日志中显示发件人成熟度信息，并与所需的过滤条件相匹配。确保您的邮件网关根据时区配置了正确的时间。

升级到 AsyncOS 14.2.x 版本后，内容或邮件过滤器、报告和邮件跟踪中的旧版 SDR 判定将替换为新的 SDR 判定，如下所示：

- 不受信任
- 可疑
- 一般
- 可靠
- 受信任
- 未知

有关针对每个新 SDR 判定的建议操作的详细信息，请参阅SDR 判定 ， 第 2 页。

有关详细信息，请参阅“思科客户连接计划”中的《思科 Talos 发件人域信誉 (SDR)》白皮书，网址为：http://www.cisco.com/go/ccp。

注释
- 您必须创建一个 Cisco 客户连接账户，才能访问 SDR 白皮书。
- 与 Cisco IPAS 争议一样，通过 Cisco 技术支持中心 (TAC) 打开支持请求来提交 SDR 争议。

SDR 判定

下表列出了 SDR 判定名称、说明和建议操作：

表 *1: SDR* 判定

判定名称	说明	建议的操作
不受信任	最差的信誉判定。 最安全的建议的阻止阈值。如果阻止阈值设置为“仅此判定”，则会看到漏报 (FN)，这会将传送的优先级确定为高于安全性。	阻止邮件。
可疑	此判定具有较低且相对安全的误报率 (FP) 可能对所有组织都不安全。 不阻止此判定确定传送的优先级高于安全性，但会导致错误的负差率。	使用邮件网关上配置的其他引擎扫描邮件。仅在审核后阻止。有关详细信息，请参阅调整发件人域信誉策略 ， 第 5 页。
一般	分配给合法和混合使用域的最常见判定，与阻止有利判定的弱指标关联。	使用邮件网关上配置的其他引擎扫描邮件。
可靠	发件人使用的是不是新域的公平域。发件人遵循发件人最佳实践，包括但不限于使用 SPF、DKIM 签名、使用 DMARC 和不发送垃圾邮件。	使用邮件网关上配置的其他引擎扫描邮件。
可信	一种极为少见的判定，表示发件人正在使用经认证的域，其中的邮件已经 DKIM 验证（在“来自：”信头域中对齐）。	允许消息。 有关如何绕过后续引擎的详细信息，请使用邮件过滤器规则（例如“skip-spamcheck”，“skip-viruscheck” 等），请参阅中的“邮件过滤器操作”部分使用邮件过滤器实施邮件策略。
未知	发件人使用 SDR 无法识别或无法用于建立信誉的域。	使用邮件网关上配置的其他引擎扫描邮件。

如何根据发件人域信誉过滤邮件

步骤	相应操作	更多信息
第 1 步	在思科邮件安全网关上启用SDR过滤。 **注释** 升级到 AsyncOS 12.0 后，默认情况下会启用 SDR 查询。	在邮件网关上启用发件人域信誉过滤，第 4 页
第 2 步	[可选] 对邮件网关中的 SDR 配置进行审查，以建立适当的SDR策略	调整发件人域信誉策略，第 5 页
第 3 步	配置邮件或内容过滤器以根据 SDR 处理邮件。	根据发件人域信誉配置邮件或内容过滤器以处理邮件，第 6 页
第 4 步	附加您配置的内容过滤器，以根据 SDR 将邮件过滤为传入邮件策略。	将内容过滤器附加到传入邮件策略，第 10 页

在邮件网关上启用发件人域信誉过滤

注释 升级到 AsyncOS 12.0 后，默认情况下会启用 SDR 查询。

过程

步骤 1 转到**安全服务 (Security Services) > 域信誉 (Domain Reputation)**。

步骤 2 点击**启用 (Enable)**。

步骤 3 选中**启用发件人域信誉过滤 (Enable Sender Domain Reputation Filtering)**。

步骤 4 （可选）如果您不希望 SDR 服务根据邮件的其他属性检查 SDR，请取消选中**包括其他属性 (Include Additional Attributes)**。

包括其他属性 (Include Additional Attributes) 会被默认启用，而 SDR 服务会根据邮件的其他属性来检查 SDR。下列其他邮件属性也将包括在 SDR 检查中，以提高效率：

- “信封发件人：”、“发件人：”和“回复收件人：”信头中出现的邮箱地址的用户名部分。
- “发件人：”和“回复收件人：”信头中的显示名称。

步骤 5 （可选）输入 SDR 查询超时前经过的秒数。

注释 修改 S查询超时值可能会影响邮件处理性能。

步骤 6 （可选）选中**基于信封发件人域匹配域例外列表 (Match Domain Exception List based on Domain in Envelope From)**：如果您希望邮件网关仅根据“信封发件人”信头中的域跳过 SDR 检查。

步骤 7 移动**范围滑块**以选择所需的 SDR 判定范围，以便在 SMTP 会话级别接受或拒绝邮件。

注释 升级到 AsyncOS 14.x 及更高版本后，范围滑块将默认指向不受信任判定。所有被判定为不受信任的邮件都会在 SMTP 会话级别被丢弃。

注释 您不能选择优先判定来拒绝邮件，因为该判定表示发件人使用的域已通过认证。

步骤 8 点击**提交 (Submit)**。

步骤 9 （可选）如果您要接受“SDR 包括其他属性协议”邮件，请点击**我同意 (I Agree)**。

注释 仅当您选择“包括其他属性”(Include Additional Attributes) 选项时，才会显示“SDR 包括其他属性协议”(SDR Include Additional Attributes Agreement) 邮件。

步骤 10 点击**确认 (Commit)** 确认更改。

下一步做什么

查看邮件网关中的 SDR 配置，以建立适当的 SDR 策略。请参阅调整发件人域信誉策略 ， 第 5 页。

调整发件人域信誉策略

SDR 为每个判定建议默认行为。但是，如果误报和误报的最佳调整对您的组织至关重要，请按照给定的步骤根据您的安全要求调整 SDR 策略。

过程

步骤 1 在邮件网关上启用 SDR，而不配置任何 SDR 策略操作10天。

步骤 2 使用邮件跟踪功能根据 SDR 判定查看邮件。

有关详细信息，请参阅在邮件跟踪中显示发件人域信誉详细信息 ， 第 10 页。您可以搜索收到判定为“不受信任”或“可疑”的邮件。

步骤 3 查看从“邮件跟踪”搜索（在步骤2中执行）中获取的邮件，查看是否存在误报或漏报。

误报是指需要传送到收件人邮箱但收到判定为“可疑”或“不可信”的邮件。漏报是指未收到“不受信任”判定，但根据与 SDR 相关的邮件属性被阻止的邮件。

步骤 4 [如果由于邮件收到“不可信”判定而出现误报]，请在继续将 SDR 策略配置为根据“不可信”判定阻止邮件之前，向Cisco TAC 打开支持请求。

注释　在大多数使用案例中，Cisco Talos希望您阻止具有“不受信任”判定的邮件。

步骤 5 如果收到“可疑”判定的邮件中存在误报，请使用建议的安全“不受信任”阈值。

注释　如果不使用“不受信任”阈值，则可以根据更具攻击性的“可疑”阈值阻止邮件。有关详细信息，请参阅根据发件人域信誉配置邮件或内容过滤器以处理邮件，第 6 页。

注释　“可疑”判定与发送垃圾邮件的大量发件人相关，但也可能传送合法（主要是低优先级）的批量邮件。根据安全要求，在审核后阻止邮件是适当的做法。

根据发件人域信誉配置邮件或内容过滤器以处理邮件

您可以使用以下任一方法中的“域信誉”邮件或内容过滤器根据SDR过滤邮件，并对此类邮件执行相应的操作：

- 发件人域判定
- 发件人成熟度
- 发件人域不可扫描

注释　从 AsyncOS 14.2.x 版本开始，发件人域有效期选项将替换为发件人成熟度。SDR 判定中已包含发件人成熟度。通常不建议根据发件人成熟度过滤邮件，特殊使用案例除外。

相关主题

- 调整发件人域信誉策略，第 5 页
- 使用邮件过滤器根据发件人域信誉过滤邮件，第 6 页
- 使用内容过滤器根据发件人域信誉过滤邮件，第 8 页

使用邮件过滤器根据发件人域信誉过滤邮件

根据发件人域判定过滤邮件

注释　建议的阻止阈值为“不受信任。”有关 SDR 判定的详细信息，请参阅SDR 判定，第 2 页，有关 SDR 策略调试，请参阅调整发件人域信誉策略，第 5 页

语法：

```
drop_msg_based_on_sdr_verdict:
if sdr-reputation (['untrusted', 'questionable'], "<domain_exception_list>")
{drop();}
```

其中：

- 'drop_msg_based_on_sdr_verdict' 是邮件过滤器的名称。
- 'sdr-reputation' 是域信誉邮件过滤器规则。
- '" 不受信任 "、" 可疑 " 是用于根据 SDR 过滤邮件的发件人域判定的范围。
- 'domain_exception_list' 是域例外列表的名称。如果不存在域例外列表，它将显示为 ""。
- 'drop' 是在邮件上应用的操作。

示例

在以下邮件中，如果 SDR 判定为“未知”，则该邮件将被隔离。

```
quarantine_unknown_sdr_verdicts:
if sdr-reputation (['unknown'], "")
{quarantine("Policy")}
```

根据发件人成熟度过滤邮件

注释 从 AsyncOS 14.2.x 版本开始，发件人域有效期选项将替换为发件人成熟度。SDR 判定中已包含发件人成熟度。通常不建议根据发件人成熟度过滤邮件，特殊使用案例除外。发件人成熟度被设为30天限制，如果超过该限制，域就会被视为邮件发件人的成熟地址，并且不会提供进一步的详细信息。

语法：

```
<msg_filter_name>
if sdr-maturity (< ‘unit'>, < ‘operator'> < ‘actual value’ >)
{<action>}
```

其中：

- 'sdr-maturity' 是发件人成熟度邮件过滤器规则。
- ‘unit' 是“天数”、“年”、“月”或“周”选项，用于根据发件人成熟度过滤邮件。
- ‘operator' 是以下比较运算符，用于根据发件人成熟度过滤邮件：
  - - >（大于）
  - - >=（大于或等于）
  - - <（小于）
  - - <=（小于或等于）
  - - ==（等于）
  - - !=（不等于）

- - 未知

- ‘actual value' 是用于根据发件人成熟度过滤邮件的编号。

示例

在以下邮件中，如果发件人的域成熟度未知，则该邮件将被丢弃。

```
Drop_Messages_Based_On_SDR_Maturity: if (sdr-maturity ("unknown", "")) {drop();}
```

在以下邮件中，如果发件人的域成熟度少于一个月，则该邮件将被丢弃。

```
Drop_Messages_Based_On_SDR_Maturity: if (sdr-maturity ("months", <, 1, "")) { drop(); }
```

根据发件人域不可扫描过滤邮件

语法：

```
<msg_filter_name>
if sdr-unscannable (<'domain_exception_list'>)
{<action>}
```

其中：

- 'sdr-unscannable' 是域信誉邮件过滤器规则。

  'domain_exception_list' 是域例外列表的名称。如果不存在域例外列表，它将显示为 ""。

示例

在以下邮件中，如果邮件未通过 SDR 检查，则该邮件将被隔离。

```
Quarantine_Messages_Based_On_Sender_Domain_Unscannable: if (sdr-unscannable (""))
{quarantine("Policy");}
```

使用内容过滤器根据发件人域信誉过滤邮件

开始之前

- （可选）创建仅包含域的地址列表。要创建一个，请转到 Web 界面中的邮件策略 *(Mail Policies)* > 地址列表 *(Address Lists)* 页面或 CLI 中的 `addresslistconfig` 命令。有关详细信息，请参阅邮件策略。
- （可选）创建域例外列表。有关详细信息，请参阅创建域例外列表，第 9 页。

过程

步骤 1 转到**邮件策略 (Mail Policies)** > **传入内容过滤器 (Incoming Content Filters)**。

步骤 2 点击**添加过滤器 (Add Filter)**。

步骤 3 输入内容过滤器的名称和描述。

步骤 4 点击**添加条件 (Add Condition)**。

步骤 5 点击**域信誉 (Domain Reputation)**。

步骤 6 选择以下任一条件以根据 SDR 过滤邮件：

- 选择**发件人域信誉判定 (Sender Domain Reputation Verdict)** 以选择判定范围，根据从 SDR 服务接收的判定过滤邮件。

  注释 建议的阻止阈值为“不受信任。” 有关 SDR 判定的详细信息，请参阅SDR 判定 ，第 2 页。

- 选择**发件人成熟度 (Sender Maturity)**，选择比较运算符，输入一个数字，然后选择根据发件人域成熟度过滤邮件的时段。

  注释 从 AsyncOS 14.2.x 版本开始，发件人域有效期选项将替换为发件人成熟度。SDR 判定中已包含发件人成熟度。通常不建议根据发件人成熟度过滤邮件，特殊使用案例除外。发件人成熟度被设为30天限制，如果超过该限制，域就会被视为邮件发件人的成熟地址，并且不会提供进一步的详细信息。

- 选择**发件人域信誉不可扫描 (Sender Domain Reputation Unscannable)** 以过滤未通过 SDR 检查的邮件。

步骤 7 （可选）选择您不希望邮件网关根据 SDR 过滤邮件的已列入允许之列的域列表。

步骤 8 点击**添加操作 (Add Action)**，配置要根据 SDR 对邮件执行的相应操作。

步骤 9 提交并确认更改。

创建域例外列表

域例外列表由仅包含域的地址列表组成。无论思科邮件安全网关上配置的邮件策略如何，您均可使用域例外列表跳过对所有传入邮件的 SDR 检查。

注释 如果要在传入邮件上跳过针对特定邮件策略的SDR内容过滤器操作，则需要在域信誉内容过滤器中选择域例外列表。

使用域例外列表的条件

如果要仅根据“信封收件人：”(Envelope From:) 信头中的域跳过SDR检查，请从“域信誉”(Domain Reputation) 设置页面中选择“基于信封发件人域匹配域例外列表”(Match Domain Exception List based on Domain in Envelope From:) 选项。

如果禁用“根据‘信封发件人:’中的域匹配域例外列表”(Match Domain Exception List based on Domain in Envelope From:) 选项，则当 `HELO:`、`RDNS:`、信封发件人：、发件人：和回复收件人：中的任何域为配置的域例外列表。

过程

步骤 1 转到**安全服务 (Security Services) > 域信誉 (Domain Reputation)**。

步骤 2 点击域例外列表下的**编辑设置 (Edit Settings)**。

步骤 3 选择仅包含域的所需地址列表。

步骤 4 提交并确认更改。

下一步做什么

您还可以在 CLI 中使用 `domainrepconfig` 命令创建域例外列表。有关详细信息，请参阅《适用于思科邮件安全设备的 AsyncOS 的 CLI 参考指南》。

将内容过滤器附加到传入邮件策略

您可以附加已配置的内容过滤器，以根据 SDR 将邮件过滤为传入邮件策略。

过程

步骤 1 转到**邮件策略 (Mail Policies) > 传入邮件策略 (Incoming Mail Policies)**。

步骤 2 点击内容过滤器下方的链接。

步骤 3 确保选择**启用内容过滤器(自定义设置) (Enable Content Filters [Customize Settings])**。

步骤 4 选择您为根据 SDR 过滤邮件而创建的内容过滤器。

步骤 5 提交并确认更改。

发件人域信誉过滤和集群

如果使用集中管理，则可以启用集群、组和计算机级别的 SDR 过滤和邮件策略。

在邮件跟踪中显示发件人域信誉详细信息

您可以使用邮件跟踪来根据 SDR 查看邮件详细信息。

开始之前

- 请确保在邮件网关上启用邮件跟踪功能。要启用邮件跟踪，请转到 Web 界面中的**安全服务 (Security Services) > 邮件跟踪 (Message Tracking)**页面。

注释 即使未在邮件网关中配置基于SDR的内容或邮件过滤器，也可以根据SDR判定跟踪邮件。

过程

步骤 1 转到**监控 (Monitor) > 邮件跟踪 (Message Tracking)**。

步骤 2 点击**高级 (Advanced)**。

步骤 3 检查邮件事件下的**发件人域信誉**。

步骤 4 根据从 SDR 服务接收到的判定，选择所需的 SDR 判定以查看邮件。

步骤 5 （可选）选中**不可扫描 (Unscannable)**，以在 SDR 检查失败时查看消息。

步骤 6 （可选）选择所需的 SDR 威胁类别，以根据威胁类别查看邮件。

步骤 7 点击**搜索 (Search)**。

查看警报

下表包含为 SDR 生成的各种系统警报的列表，包括对警报和警报严重性的说明。

组件/警报名称	邮件和描述	参数
MAIL.IMH.SENDER_DOMAIN_LOOKUP_FAILURE_ALERTS	SDR 查找失败。原因 - <$reason> 警告。当SDR查询失败时发送。	‘**reason**’ - SDR 查询失败的原因。

查看日志

SDR 过滤信息将发布到邮件日志。大多数信息处于“信息”或“调试”级别。

SDR 过滤日志条目的示例

SDR 过滤信息将发布到邮件日志。大多数信息处于“信息”或“调试”级别。

- 发件人域信誉请求超时，第 11 页
- 发件人域信誉常规错误，第 12 页

发件人域信誉请求超时

在本示例中，日志显示了由于与 SDR 服务通信时出现请求超时错误而未根据 SDR 过滤的邮件。

```
Mon Jul 2 09:00:13 2018 Info: New SMTP ICID 4 interface Management (192.0.2.10) address
224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 09:00:13 2018 Info: ICID 4 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 09:00:13 2018 Info: Start MID 4 ICID 4
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 From: <sender1@example.com>
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 09:00:13 2018 Info: MID 4 Subject 'Message 001'
Mon Jul 2 09:00:13 2018 Info: MID 4 SDR: Message was not scanned for Sender Domain Reputation.
 Reason: Request timed out.
```

解决方案

当 SDR 请求超时时，邮件会被标记为不可扫描，并且配置的操作将应用于邮件。

发件人域信誉常规错误

在本示例中，日志显示了由于未知错误而未根据 SDR 过滤的邮件。

```
Mon Jul 2 09:00:13 2018 Info: New SMTP ICID 4 interface Management (192.0.2.10) address
224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 09:00:13 2018 Info: ICID 4 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 09:00:13 2018 Info: Start MID 4 ICID 4
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 From: <sender1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 09:00:13 2018 Info: MID 4 Subject 'Test mail'
Mon Jul 2 09:00:13 2018 Info: MID 4 SDR: Message was not scanned for Sender Domain Reputation.
 Reason: Unknown error.
```

解决方案

发生未知错误时，邮件会被标记为不可扫描，并且配置的操作会应用于邮件。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。