什么是最佳实践为使用SenderBase ？

目录

简介

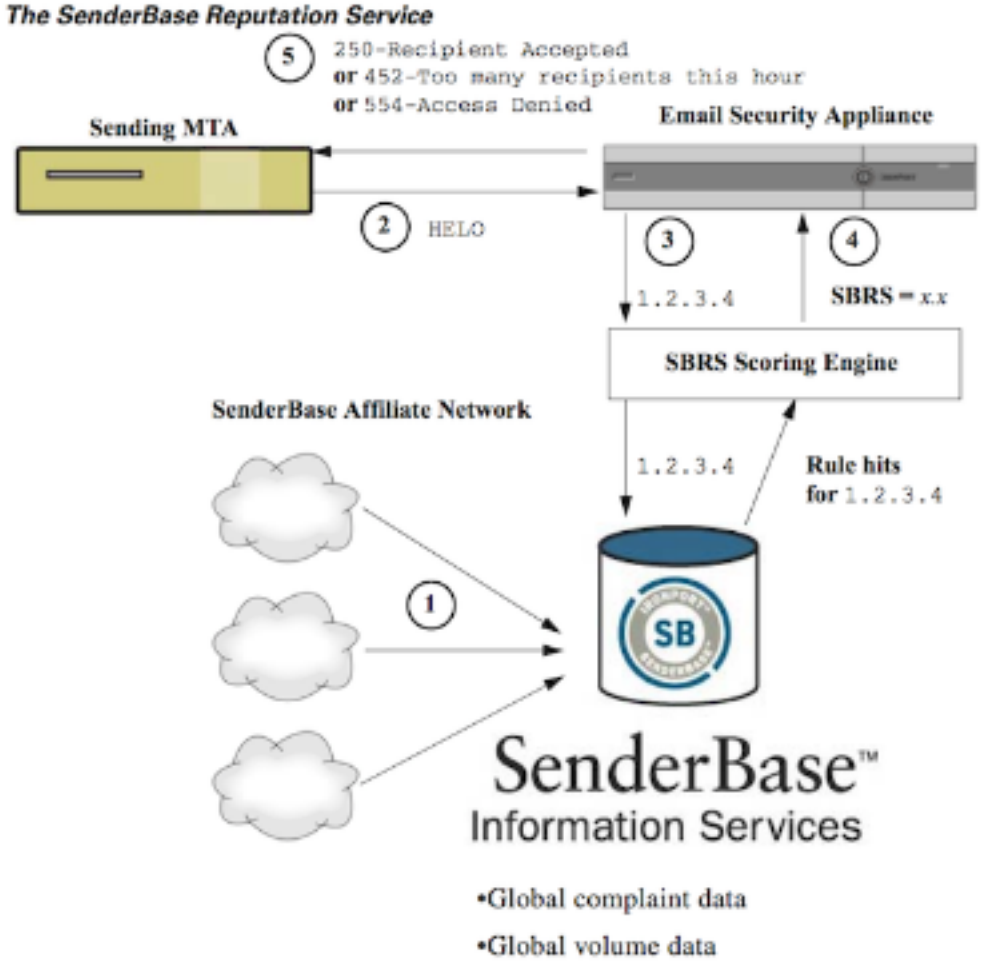
本文描述最佳实践为使用SenderBase。

什么是最佳实践为使用SenderBase ？

SenderBase名誉服务(SBRS)为您提供一准确，灵活的方式拒绝或节流怀疑的系统传送根据远程主机的连接的IP地址的垃圾邮件。SBRS返回根据可能性的分数从指定源的一个消息是垃圾邮件，范围自-10 (无疑是垃圾邮件)通过0到+10 (无疑不是垃圾邮件)。 虽然SBRS可以使用作为一独立反垃圾邮件解决方案，最有效，当与一基于内容的反垃圾邮件扫描仪结合。

SenderBase分数可以用于在SMTP监听程序的主机访问表(帽子)映射对不同的发送方组的流入SMTP连接。 每发送方组关联与它影响的策略流入电子邮件如何被处理。 执行与SenderBase分数完全地是对拒绝邮件，或者节流怀疑的垃圾邮件发送方的最普通的事。

您在帽子能使用SBRS分数拒绝或节流电子邮件。您能也创建消息过滤器指定“阈值” SBRS分数的能进一步操作在已处理由系统。下图所示提供一概略的概述SBRS分数如何可以用于阻塞或节流怀疑的发送方：



1. SenderBase子公司发送实时，全局数据。
2. 发送MTA开放连接用设备。
3. 设备检查全局数据连接的IP地址。
4. SenderBase名誉服务计算此消息是垃圾邮件的可能性并且分配SenderBase名誉斯克尔。
5. 设备返回根据SenderBase名誉(任一拒绝的电子邮件或限制的发送方)的答复斯克尔。

您如何使用SBRS分数将依赖于怎样积极您要是在PRE过滤电子邮件。电子邮件安全工具(ESA)提供实现的SenderBase三个不同的策略：

- **保守主义者**：保守的方法比-7.0将阻塞与SenderBase名誉斯克尔的消息更低，节流在-7.0和-2.0之间，运用在-2.0和+6.0之间的默认策略和申请委托策略与分数极大消息比+6.0。使用此方法保证一最近的零的错误肯定速率，当完成更加好的系统性能时。
- **一般**：一一般方法比-4.0将阻塞与SenderBase名誉斯克尔的消息更低，节流在-4.0和0之间，运用在0和+6.0之间的默认策略和申请委托策略与分数极大消息比+6.0。使用此方法保证一非常小错误肯定速率，当完成更加好的系统性能时(因为更多邮件转轨远离处理的反垃圾邮件)。
- **积极**：一积极的方法比-1.0将阻塞与SenderBase名誉斯克尔的消息更低，节流在-1.0和0之间，运用在0和+4.0之间的默认策略和申请委托策略与分数极大消息比+4.0。使用此方法，您也许导致一些错误肯定;然而，此方法通过转轨远离反垃圾邮件处理的多数邮件最大化系统性能。

下面的图表和的表汇总这三项策略：

Approach	Characteristics	Whitelist	Blacklist	Suspectlist	Unknownlist
		Sender Base Reputation Score range:			
Conservative	Near zero false positives, better performance	7 to 10	-10 to -4	-4 to -2	-2 to 7
Moderate (Installation default)	Very few false positives, high performance	Sender Base Reputation Scores are not used.	-10 to -3	-3 to -1	-1 to +10
Aggressive	Some false positives, maximum performance. This option shunts the most mail away from Anti-Spam processing.	4 to 10	-10 to -2	-2 to -1	-1 to 4
		Mail Flow Policy:			
All approaches		Trusted	Blocked	Throttled	Accepted

实现限制的SenderBase或阻塞

使用SenderBase分数的最佳方法含义跟随一简单，两部分方法。 首先，您决定您的策略(例如，您可能从以上“保守的”的策略开始)并且映射策略给发送方组。然后，您映射那些发送方组对您希望的策略。ESA已经创建的发送方组和邮件流量策略矩阵能起一个模板作用对于您的SBRS的实施。

要实现SenderBase限制基于默认策略，您将编辑四发送方组(Whitelist，黑名单， Suspectlist和Unknownlist)在邮件策略>主机访问表(帽子)概述。 开始通过单击在“Whitelist”发送方组。 然后，使用在发送方选项卡的下拉菜单，请单击“添加发送方”有“SenderBase名誉的斯克尔(SBRS)”选择。 这将添加一条SBRS线路到发送方列表。 填写您的SBRS分数范围(在这种情况下6.0到10.0)并且点击**SUBMIT按钮**。

Whitelist发送方组的策略是“委托。”默认情况下，此策略将跳过处理的反垃圾邮件，将增加系统性能。 由于有非常高SBRS分数的发送方是非常不可能发送垃圾邮件，单独此步骤将增加吞吐量。根据下面表编辑剩余的三个发送方组添加SBRS分数， ：

发送方组	斯克尔范围	结果
Whitelist	6到10	已知好发送方不会被扫描
Unknownlist	-2到+6	有一点信息的发送方通常将被扫描
Suspectlist	-7到-2	他们能发送有恶劣的名誉的发送方将大量地被节流减少相当数量垃圾邮件
黑名单	-10到-7	从已知垃圾邮件发送者的邮件将拒绝在与5xx答复的SMTP时间

当执行添加分数范围时的您，请勿忘记点击"Commit Changes."当您增加SBRS计分的规则到存在发送方组时，请在发送方列表的底部放置他们在任何组中。 请定购事态，当定义在监听程序的帽子时的发送方组，作为组从顶向下被评估，并且在每组内，每个规则单个被评估，从顶向下。 在帽子中，匹配发送方的第一个规则将用于选择策略。如果从一个发送的域的一流入连接有一个确定SBRS分数并且匹配在一个规则的范围在监听程序的帽子，邮件流量策略将应用，即使在发送方组列表的其他规则进一步下来也许也配比。

如果您的放的发送方策略到发送方组要求所有非SBRS规则被评估，在SBRS分数考虑前，则您能特

别地添加在现有发送方组结束时列表SBRS策略的匹配与他们的相关策略一起的四新的发送方组。

相关信息

- SenderBase常见问题
- 技术支持和文档 - Cisco Systems