

SenderBase使用哪些类型的阻止列表？

目录

[简介](#)

[SenderBase使用哪些类型的阻止列表？](#)

[相关信息](#)

简介

本文档介绍SenderBase使用的阻止列表类型。

SenderBase使用哪些类型的阻止列表？

SenderBase信誉服务(SBRS)提供了一种准确而灵活的方法，让您可以根据远程主机的连接IP地址拒绝或限制疑似传输垃圾邮件的系统。SBRS根据来自给定来源的邮件是垃圾邮件的概率返回分数，范围从-10（肯定是垃圾邮件）到0到+10（肯定不是垃圾邮件）。

任何IP地址的SBRS得分的一个重要组成部分是其在其他基于DNS的阻止列表上存在。SBRS使用24个不同的基于DNS的阻止列表（以不同方式加权）来提高SBRS得分。某些阻止列表（如SORBS）实际上有多个与它们关联的列表，具体取决于系统在其数据库中列出的原因。SBRS评分还有其他组件，例如关于IP地址和邮件量的投诉级别，但是SBRS评分算法中使用的确切组件和阻止列表的权重会随着时间的推移而改变，并且是专有的。

SenderBase使用的基于DNS的主要阻止列表“系列”包括：

- 垃圾邮件警察：www.spamcop.net
- SBL（SpamHaus阻止列表）：<https://www.spamhaus.org/sbl/>
- PBL（Spamhaus策略阻止列表）：<https://www.spamhaus.org/pbl/>
- SORBS(垃圾邮件和开放式中继阻止系统)：www.sorbs.net
- OPM（打开代理监控器列表）：www.blitzed.org
- CBL（复合阻止列表）：cbl.abuseat.org
- 5-10阻止列表：www.five-ten-sg.com
- MAPS(Trend Micro DNSBL):<https://www.ers.trendmicro.com/>

相关信息

- [SenderBase常见问题](#)
- [技术支持和文档 - Cisco Systems](#)