
SecurityGateway®
This program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program or any portion of it, may result in severe criminal and civil penalties, and will be prosecuted to the maximum extent possible under law.
Copyright © 1996-2025 MDaemon Technologies, Ltd.
MDaemon® and related trademarks are the property of MDaemon Technologies, Ltd. and are registered and/or used in the U.S. and countries around the world. All trademarks are property of their respective owners.
MDaemon®
technologies

管理员手册

v11.0

SecurityGateway for Email Servers
管理员手册

v11.0.0 - July 2025

目录

章节

1 SecurityGateway

1.1 概述

MDaemon Technologies 作为邮件服务器技术方面的专家，成立多年来一直致力于发展邮件安全防火墙，用于任何 SMTP 邮件服务器的用户。SecurityGateway for Email Servers 合并多个防御层，为您的网络边缘提供全面的保护，以阻止垃圾邮件，网络钓鱼，病毒以及其他对您邮件通信产生的威胁。建立于行业标准的 SIEVE 邮件过滤语言，SecurityGateway for Email Servers 邮件安全防火墙在管理接收与外发的邮件数据流方面具有极高的性能与极强的灵活性。

SecurityGateway 邮件安全防火墙提供许多优势：

- **准确检测——**SecurityGateway 具有多种分析工具，可以将合法邮件与各种威胁隔离，它重用最好的已经证明的反垃圾邮件 125，反病毒 146，反诈骗 148，以及反滥用 172技术以达到 99% 的垃圾邮件阻止率与近零的误报率。
- **简单管理——**一个直观的，具有任务导向特色的界面为 SecurityGateway 的每个主要部分提供了一个*登陆界面*。这些登陆页面包含了常见任务的列表，并提供了通往各个页面的链接，您可以在这些页面上执行任务。这个方法可以帮助管理员 50最省力地执行常规操作。此外，可以指派域管理员具有管理权限，允许该管理员管理一个或多个由全局管理员指定的域。不仅如此，授权终端用户 28可以不必联系管理员直接对邮件进行各种处理。
- **防止数据丢失——**除了过滤接收的邮件数据流，SecurityGateway 还能过滤外发的邮件。界面简单易用，允许您创建策略以检测与阻止来自您网络外部那些敏感信息未经认证的传输。
- **强大的过滤引擎——**SecurityGateway 强大的过滤引擎基于 SIEVE 邮件过滤语言。此外，使用包含其内的邮件内容过滤 195与SIEVE 脚本编辑器 219，管理员可以通过编辑他们自己的 SIEVE 脚本来扩展 SecurityGateway 的功能。
- **详细报告——**使用 SecurityGateway 的详细报告 266以识别邮件数据流模式和可能存在的问题。所有报告都支持即点即到与深入式地获取目标文件，允许执行进一步分析。
- **灵活的防御层**——希望在 SecurityGateway 多个防御层中调整其执行顺序的管理员，具有充分的灵活性以针对他们独特的邮件模式优先考虑安全规则。

功能概述

左窗格中的 SecurityGateway 的导航菜单包含六个菜单，每个菜单都对应一部分 SecurityGateway 的功能。以下是对这六个主要部分的简单概述：

主页

The Dashboard

您登录 SecurityGateway for Email Servers的第一个页面是 "仪表板"，位于主页菜单下方。该仪表板可以让您快速地概览 SecurityGateway 的当前状态与一些关于其近 24 小时内活动的摘要报告[266]。

仪表板顶部是*服务器状态*部分。该部分告诉您 SMTP 会话是否运行，并提供您可以启动或停止会话的链接。此外，控制面板列出了您的注册码大小，提供链接来管理您的注册[121]与激活，并列出了当前存在的域与用户数。它还提供了通往域列表[41]的链接以管理您的域和用户。在软件更新[120]可用时，本节还将提供有关更新的详细信息的链接。然后，将显示 SMTP 入站和出站会话的活动会话数，并且 "队列状态"部分将列出入站、投递和坏邮件队列中的邮件数。在同一部分中，对于全局管理员，还列出了 "管理员和用户隔离"中的邮件数。此外，在 "入站和投递队列"的条目中，有一个选项可以冻结/解冻每个队列。在*服务器性能*部分中，"全局管理员"可以查看 "可用磁盘空间"总量。然后，将显示系统和 SecurityGateway 的 CPU、物理内存和虚拟内存统计信息、IKARUS[146]、ClamAV[146] 和 SpamAssassin[129] (SpamD[131]) 进程。

"服务器状态"部分下是*"服务器统计"*部分。该部分显示了 SecurityGateway 的六个图表报告：接收 vs. 外发邮件[266]，邮件占用的总带宽[266]，合法 vs. 垃圾邮件[266]，垃圾邮件分析[266]，顶级邮件收件人[267]，与顶级垃圾邮件域[268]。每个报表都显示了近 24 小时内的统计数据。如果您希望更改要显示的报告，或创建新报告和自定义报告进行显示，请点击**自定义图表**。最后，报告和自定义图表具有元素，您可以将指针悬停在这些元素上，来查看有关这些元素的详细信息。对于自定义图表，您还可以通过单击图表数据点向下挖掘关联的邮件日志条目。

域管理员[50]将只能看到他们具有管理权限的域的统计信息和选项。

我的账户

在主页菜单下方的是您的我的账户[28]选项，允许您管理自己的账户设置、隔离、邮件日志和搜索邮件归档。

设置/用户[40]

*设置/用户*菜单有7个分支部分，包含链接通往 SecurityGateway 的核心配置选项。您将使用这些部分中的选项以设置您的域与用户账户、邮件投递选项、隔离设置、备份与数据库首选项，以及其他一些配置选项。设置/用户菜单有三个分支部分：

- 账户[41]—— "账户"部分位于 *"设置/用户"*菜单之下，包含了关于您的 SecurityGateway 用户账户与域的选项。该部分之下有五个与账户相关的链接，它们包括一些选项用于创建域与用户账户，指定用户验证来源，为一系列用户选项设置默认值等等。
- 邮件配置[65]——邮件部分提供链接通往五个页面，用于管理各种与邮件相关的功能。例如，您将使用这部分的选项来指定您用户的邮件账户所位于的服务器，设置您的隔离区选项，配置各种邮件投递选项以及管理其他的技术性设置。

- 免责声明(页眉/页脚)[95]——邮件免责声明是服务器可以动态添加到入站、出站和本地邮件正文上方或下方的文本部分。使用该页面来创建和管理您的免责声明。
- 系统[100]——系统部分位于*"设置/用户"*菜单之下,包含链接通往各种系统功能页面,比如加密设置,HTTP 界面选项,目录位置,磁盘空间管理选项等等。
- 数据库维护[115]——这部分的选项处理 SecurityGateway 保存的数据类型与数量,有自动备份选项,还有些选项用于自备份文件恢复服务器。
- 注册[121]——注册页面列出了您的产品注册信息,包括注册该产品的人名或公司,注册码以及您注册的状态。

要了解更多详情,请参见这部分的概述或每一部分下的各个页面。

安全[124]

*安全*菜单有八个部分,具有各种工具以帮助您保护您的域与用户免受垃圾邮件,病毒,邮件滥用以及其他安全风险的侵扰。以下是对各个安全部分的简单概述。要了解更多详情,请参见各个部分。

- 反垃圾邮件[125]——反垃圾邮件部分位于安全菜单之下,包含一些选项帮助您防范垃圾邮件或主动发送的垃圾邮件。在这部分下方列出了九个反垃圾邮件功能,包括通过使用启发式、贝叶斯分析、DNS、URI 阻止列表和灰名单等来识别和防止垃圾邮件的选项。
- 反病毒[146]——反病毒部分位于安全菜单之下,包含一些选项以帮助您识别受病毒感染的邮件并防范它们侵扰您的用户。为提供周密的病毒防护,SecurityGateway 支持两种反病毒引擎:Clam AntiVirus (ClamAV™) 和 IKARUS Anti-Virus。ClamAV 是专门为邮件网关设计的开源 GPL)防病毒工具包。IKARUS Anti-Virus 提供可靠的保护来使用户免受恶意软件和潜在敌对程序的侵扰。它整合了传统的病毒防护方法和最新的预防性技术。SecurityGateway 还包含爆发保护[126],提供了一个额外的保护层来防止病毒爆发。
- 反诈骗[148]——反诈骗部分具有一些工具,可以帮助您识别来自伪造的或者"欺诈性"地址的邮件。该部分下有六个反诈骗功能,比如 DKIM 验证、发件人 ID、回呼验证等。
- 反滥用[172]——反滥用部分包含一些工具,可以帮助您防范其他人滥用或者不恰当地使用您的邮件系统来中继垃圾邮件,防止其他人占用大量的带宽,或过于频繁地连接您的服务器等等。反滥用部分下有六个工具。
- **过滤**——过滤部分包含两个功能:邮件内容过滤[195]与附件过滤[203]。"邮件内容过滤"页面可以用来创建过滤规则以执行一系列操作。您可以创建规则以拒收满足某种条件的邮件,复制邮件或将邮件重新指向不同的地址,隔离邮件等等。附件过滤页面上的选项可以用于指定当邮件具有某一特定类型的附件时,将阻止或隔离该邮件。您可以全局性地或为每个域定义过滤限制。
- 阻止列表[205]—阻止列表是您希望阻止或隔离的电子邮件、主机和 IP 地址列表。默认情况下,那些邮件将在 SMTP 会话中被拒收,但是在"阻止列表操作"页面,您可以更改这项设置以隔离邮件。可以全局也可以为特定的域设置将采取的措施,并且阻止列表本身也可进行全局或特定域的设置。
- 允许列表[212]—允许列表是您希望免于一些安全限制的电子邮件、主机和 IP 地址列表。启发式与贝叶斯、DNSBL、DKIM 验证以及 SecurityGateway 中几乎每一个其他的安全功能,都具有选项用于在发件人,主机,邮件等显示在适当的允许列表上时,将它们从中排除。每个允许列表都可以进行全局或特定域的设置。

- **Sieve Scripts**[219]—SecurityGateway 使用 Sieve 电子邮件过滤语言来执行其许多功能，而 Sieve Scripts 页面可供您查看这些功能的执行顺序。它还为您提供了 Sieve 脚本编辑器以让您可以用之创建您自己定制的脚本。

邮件/队列[254]

邮件/队列菜单为您提供两部分的设置：

- 邮件日志[254]——邮件日志针对您用户发送与接收的每封邮件，都会包含一个条目。它列出了邮件的处理日期和时间，发件人和收件人，以及邮件主题。此外，还列出了投递结果，如是否被投递、隔离或拒绝，若未投递还会提供原因，如发件人被列入阻止列表，邮件包含受限制的附件等等。日志中的每个条目还会列出邮件的大小与其邮件总值[143]。根据邮件日志，您可以查看每封邮件的详情，包括其投递的详情和邮件的内容与总值（可用时）。您还可以将邮件标记为垃圾邮件或非垃圾邮件，这有助于改进 SecurityGateway 的贝叶斯学习功能并更准确地对邮件进行分类。
- **邮件队列**——该部分提供一些链接，通往四个不同的邮件队列：用户隔离区，管理隔离区，邮件等待投递队列，与坏邮件。用户隔离区[255]是一个指定的保持队列，用于那些没有通过某些安全功能的接收邮件。用户可以登录到 SecurityGateway 查看他们隔离文件夹的内容，并从中选择以查看邮件，删除邮件或为它们解除隔离状态以便进行正常投递。管理隔离区[256]与用户隔离区类似，但是它针对的是外发邮件与含有病毒的邮件。只有管理员才能访问管理隔离区。等待投递队列[257]是一个队列，针对所有等待投递的邮件，包括那些无法投递的邮件与当前处于重试系统的邮件。您可以从该页查看队列中的任何邮件，将邮件退回至其发件人，停止邮件的投递，或者立即重试投递队列中的一封选中邮件或所有邮件。坏邮件[258]队列是针对那些因为发生致命处理错误而无法进行投递的邮件，比如一封邮件在递归循环中被捕获，使之达到*最大邮件跳跃计数*[78]。您可以从坏邮件队列查看队列中的任何邮件，可以设法将邮件退回至其发件人，删除邮件，或者立即重试投递队列中的一封选中邮件或所有邮件。

日志[260]

日志菜单帮助您访问以下三部分：

- 邮件日志[260]——这是在以上的邮件/队列部分之下，又一个可以访问邮件日志论述的链接。在两个地方都有提供只是为了管理员的方便。
- 日志文件[261]——您可以使用日志文件部分来查看 SecurityGateway 保存在您日志文件夹[109]中的各种日志文件。不像邮件日志，日志文件并不存储在数据库中，因此也不向每种事件提供可保存的列表与独立的条目。取而代之的，它们只是纯文本文件，记录各种 SMTP 连接与其他 SecurityGateway 执行的功能。所有日志文件的页面位于日志文件部分之下，列出了包含在您日志文件夹中的所有日志文件，包括当前的日志文件与翻转[262]日志文件。您可以从那页面查看所有列出的文件。日志文件部分的其他页面提供了可以查看 SecurityGateway 当前日志文件的快捷方式，例如系统日志、接收与外发日志、病毒库更新日志等等。
- 配置[262]——配置部分提供了一条链接，通往日志配置页面，用于配置您日志的首选项与选项。在该页您可以根据您的需要指定在接收，发送与 HTTP 日志中，那些将写入的数据的详细程度。您还可以选择将被创建的日志文件的类型。标准设置，每天一个新设置且将日期并入文件名，或者每天一个新设置且将星期几并入文件名。最后，您可以选择各种日志文件维护设置，比如在保存文件前与新建文件前的大小规定，可以创建的“翻转”文件的数量，文件在归档前可以存在的时间长短等等。

报告 266

报告部分提供了互动而详尽的关于 SecurityGateway 行为的图表报告。您可以产生显示接收邮件数量较之外发邮件数量的报告，对接收的垃圾邮件类型进行分析的报告，带宽的报告，根据累积邮件大小而排出的顶级发件人的报告，病毒报告等等。此外，每个报告还提供选项，允许您指定报告的参数。比如，您可以指定报告中的数据用于特定的域或所有的域；按小时、天数，月数来数绘制数据；报告的数据采集还包括了固定的时间周期，比如一天、一周、一个月或使用一段您指定的日期。不仅如此，每个报告之下还有一个细目表，对报告内容作了分析，还提供了链接通往邮件日志，日志将被过滤以显示仅与报告中的该条目相关的数据。比如，它提供了链接以显示在指定的小时内列在报告上的所有接收邮件，在某一天收到的所有包含病毒的邮件，一个域中的顶级收件人收到的所有邮件等等。

系统要求

要了解最新的 SecurityGateway 系统配置要求与推荐，请参见：SecurityGateway for Email Servers - 系统要求在 www.mdaemon.com 中列出。

获得帮助

请访问www.mdaemon.com/Support/来获得 SecurityGateway 最新的技术支持与帮助选项，包括：电话支持、邮件支持、知识库、常见问题解答和社区论坛等。

SecurityGateway 11.0.0 - July 2025

1.2 版本 11.0 新功能

特殊说明事项

已将数据库更新到 Firebird 5.0。此更新要求将数据库文件转换为 Firebird 5.0 格式。

- 此转换过程将在安装过程中自动执行，取决于数据库的大小和存储它的磁盘的性能，可能需要几分钟时间才能完成。在此期间，SecurityGateway 将不可用。
- 在更新之前，将创建数据库文件的备份。名为 SecurityGateway.fb3 的备份文件将被保存在 SecurityGateway\App 目录下。
- 请注意，一旦更新了数据库文件，它将不再与早期版本的 SecurityGateway 兼容。

新功能

AI 分类 238

新增 AI 分类功能，充分利用人工智能来分析电子邮件内容，并根据可配置的条件对邮件进行分类。

- 管理员可以配置来自多个提供商的 AI 模型，包括 OpenAI/ChatGPT、Google Gemini 以及自定义的 API 终端。该系统允许使用邮件数据变量来创建自定义的 AI 提示词，以便让 AI 将邮件分类到管理员预设的类别中。分类规则可用于根据 AI 的分类结果触发特定的操作。

- 任何支持 OpenAI API 格式的模型都可以使用，包括在您自有基础设施上运行的本地模型。用户需自行获取所需的 API 密钥，并自行承担使用第三方 AI 服务所产生的费用。
- AI 分类提供了一种先进的方法，用于识别复杂的网络钓鱼攻击、检测诸如个人身份信息 (PII)等敏感内容，并过滤传统规则可能遗漏的垃圾邮件。

在登录到 SecurityGateway UI 时，Microsoft 365 用户验证源[55]现在支持 OAUTH Authorization Code Flow 。

该方式更安全，并允许使用 Microsoft 365 双重验证。在将用户的域配置成使用 Microsoft 365 用户验证源时，会将用户重定向到 Microsoft 365 验证 URL 来完成登录流程。一旦成功登录到 Microsoft 365，会将用户的浏览器重定向回 SecurityGateway。

注意：SMTP 验证仍然只支持 "Resource Owner Password Credentials Grant (身份信息透传授权)"验证流，它不支持双重验证。

其他功能和变更

- 自定义仪表板图表[28]现在支持向下挖掘。双击一个图表元素来查看相应的邮件。
- 在编辑一名用户时，现在会指示是否设置了本地密码。已新增选项来清除本地密码(若存在)。没有本地密码的用户只能使用支持其域验证的用户验证源[48]来进行验证。不再为新建的用户分配随机强密码。
- 邮件日志中的 IP 地址栏现在按八位组 (octet) 排序 IPv4 地址，而不是按字符串排序。
- 已将从 "Office 365"至 "Microsoft 365"的所有引用更新为符合 Microsoft 的当前品牌。
- 已为管理界面 HTTP 服务器实施 HTTP/1.1 始终保持活动状态。
- 已为管理界面 HTTP 服务器实施 HTTP/1.1 gzip 内容编码。
- 已将 SG-API.html 文件中的链接更新为指向更新过的 XML-RPC 资源。
- 新增了 Sieve 变量 ${vnd.mdaemon.execute.exit_code}，用于获取通过执行 Sieve 命令[230]的进程的退出代码。该变量仅在 execute 命令执行完成后可用。

  使用示例：

```
require ["variables", "securitygateway"];


execute "some-script.bat";


if string "${vnd.mdaemon.execute.exit_code}" "1" {
 fileinto "spam";
} elsif string "${vnd.mdaemon.execute.exit_code}" "2" {
    reject "This message looks like spam";
}
```

- 已将 ClamAV[146] 更新到 1.4.2 版本。

- 已将 SpamAssassin 129 更新到 4.0.1 版本

有关变更和问题修复的完整列表，请参阅 "Windows 开始菜单"下 SecurityGateway 程序组中的发布说明。

版本 10.5 的新功能

特殊说明事项

- 不再支持使用 Microsoft Internet Explorer 来访问 "管理控制台"。请使用最新版本的 Microsoft Edge、Firefox、Chrome、Safari 或现代的移动浏览器。

新功能

The Authenticated Received Chain (ARC)

ARC 是一种电子邮件身份验证协议，允许中间邮件服务器对邮件的身份验证结果进行数字签名。当下游邮件服务器执行 DMARC 验证，并检测到 SPF 或 DKIM 失败（例如，由于转发或邮件列表修改）时，它可以查看来自可信服务器的 ARC 结果，以确定是否接受邮件。

可以在安全 | 反欺诈 | DMARC 验证 162 中配置 ARC 验证，而且在默认情况下可用。可信 ARC Sealer 是您信任其 ARC 结果的域。在进行 DMARC 验证时，将忽略来自不可信域的 ARC 结果。

可以在安全 | 反欺诈 | DKIM 签名 155 下启用 ARC 签名。不是来自本地域的邮件有资格进行 ARC 签名，并且 ARC 签名使用与 DKIM 签名相同的选择器。默认情况下禁用 ARC 签名。

有关 ARC 协议的更多信息，请参阅：RFC 8617: The Authenticated Received Chain (ARC) 协议.

搜索设置

现在，在页面顶部的标题工具栏上有一个 "搜索设置"链接。此功能可用于更轻松地查找 SecurityGateway 中许多设置和页面。只需开始输入您要查找的设置或页面中包含的单词，下方将列出指向包含这些位置的链接。此功能可供管理员和用户使用，但不包括 "安全邮件"收件人。

已改善的 DKIM 选择器管理

新增对于共享/全局选择器 156 的支持，可用于多个域。

现在可以通过选择共享/全局选择器作为默认值来全局启用 DKIM 签名。这需要为每个域创建指向选择器公钥的 DNS 记录。

新增能够导入和导出选择器的功能。

位置数据增强

发件人 IP 地址的国家和洲现在存储在数据库中。这些字段可以在邮件日志 260 中显示为可选的列，并在查询 "邮件日志"时用作搜索条件。

新的报告[266]引入了：摘要 | 垃圾邮件 - 国家排行，入站电子邮件 | 国家排行，反垃圾邮件 | 国家排行

在创建“自定义仪表板报告”时，可以使用位置数据。

新增隔离区管理员[51]角色。

此角色允许用户配置为管理和（可选）查看用户隔离队列中的邮件，而不允许更改任何设置。

其他功能和变更

- 已在邮件日志[260]中将连接 IP 地址添加为可用的列。
- LetsEncrypt 将更改 HTTP 主机名和 AlternateHostNames(备用主机名)，以使用所有小写字符。
- 在“自定义仪表板报告”中新增一个选项，以“显示 Y 属性的前 X 名”
- 已为主机阻止列表新增默认值（"localhost"、"friend"、"user"、"ylmf-pc"、"-*"、"*_*"、"#.#.#.#"、"*.invalid"、"*/*"、"*|*"）。这些主机名通常与僵尸网络关联。
- SPF 检查行为更新：当反向路径（MAIL FROM）为 null 时，SPF 检查现在将使用 EHLO/HELO 域值进行验证，前提是它是一个有效的域。

有关变更和问题修复的完整列表，请参阅“Windows 开始菜单”下 SecurityGateway 程序组中的发布说明。

版本 10.0 的新功能

新功能

- 新增为管理仪表板[28]创建自定义图表/报告的功能。
- 已向管理仪表板[28]新增 CPU 和内存计数器，用于 SecurityGateway、SpamAssassin、Ikarus AV 和 ClamAV 进程。
- QR 码检测[182] - SecurityGateway 新增“反滥用”选项来提供抵御 QR 网络钓鱼（也叫做 QRshing 或 Quishing）的选项。当 SecurityGateway 发现附加到邮件的 QR 码图像时，邮件可以被拒收、隔离或接受，但用文本标记并调整其邮件分值。
- 加密[100]页面的“选择证书”部分现在包含一个“配置 Let's Encrypt”按钮，这将打开 Let's Encrypt PowerShell 更新[106]页面。此项允许您自动执行从 Let'S Encrypt 下载 SSL 证书的 PowerShell 脚本。Let'S Encrypt 是一个通过自动化流程提供免费证书的证书颁发机构。这旨在简化手动创建、验证、签名、安装和续订证书的传统复杂过程。
- 新增 Abusix Mail Intelligence[145] 支持（安全 | 反垃圾邮件 | Abusix），这是实时 DNS 阻止列表[134]套件。Abusix Mail Intelligence 需要 Abusix 提供的有效订阅和使用密钥。

其他功能和变更

- 加密[100]页面拥有一个新选项：*自动检测并激活更新的证书*。启用此选项后，系统将在其夜间维护过程中执行检查。对于每个活动证书，它将检查以查看：系统上是否有另一个证书稍后到期，它是否针对相同的主机名，以及它是否包括所有备用主机名。如果存在这样的证书，系统将自动激活此证书。当系统上有自动更新证书的调度任务时，例如 Let's Encrypt[104]，特别有用。默认情况下启用这个新选项。
- 在被配置为使用的 SSL 证书[103]要过期时，会向全局管理员发送一封警告电子邮件。
- 安全邮件收件人[91]可以使用登录页面上的忘记密码[92]链接，即使他们未完成设置过程也是如此。在此情况下，将重新发送账户设置邀请邮件。
- 新增日志文件[261]"*-FailedAuth.log"，用于记录失败的验证尝试。
- 已为新安装更新了默认的待阻止附件[203]列表。新增操作链接"阻止建议的文件"，允许将这些扩展应用于升级的安装。
- 现在，位置屏蔽[178]选项"接受 SMTP 连接，但阻止身份验证"是按国家的选项，而不是全局选项。阻止 SMTP 连接可防止您的服务器接收来自某个国家/地区的邮件。允许禁用验证的 SMTP 连接可让您的服务器接收来自某个国家/地区的邮件，同时阻止来自这些国家/地区的暴力/字典攻击。
- 由一个国家的位置屏蔽[178]策略阻止身份验证时，不会通告 ESMTP 对 AUTH 的支持。
- 已将 Acme-PS PowerShell 模块更新到 1.5.9 版本，该模块由 Let's Encrypt PowerShell 脚本使用。
- 域的 SMTP AUTH 密码[43]现在将匹配任何该域的用户，时机是使用 SMTP 验证[175]要求*"身份验证凭证必须与电子邮件发件人的凭证匹配"*。
- 在"访问控制"下新增一个用户选项[60]，用于"允许用户查看邮件记录"。如果禁用此项，只有管理员可以查看其邮件日志[38]或隔离区[37]中的记录详细信息。默认情况下，此选项对升级启用，但对新安装禁用。
- 新建/编辑管理员[51]页面包含一个新选项："可以查看域用户邮件的来源"。该选项根据您的数据保留[116]设置，应用到 SecurityGateway 已保留的邮件。将始终保留排队等待投递到域邮件服务器[66]的邮件和已隔离[71]的邮件。此项不应用于已归档[78]的邮件。
- SMTP 验证[175]页面有一个新选项："不允许在 SMTP 端口上进行验证"。如果 SMTP 客户端提供了 AUTH（验证），则不会在 EHLO 响应中提供 AUTH，并且会将 AUTH 视为未知命令。此设置在所有合法账户都使用 MSA[76]或其他端口来提交经过验证的邮件的配置中很有用。在这种配置中，假定在 SMTP 端口上进行任何验证的尝试都必须来自攻击者。
- 增加了"邮件信息"（查看邮件）窗口的默认大小。
- 已将 ClamAV 更新到 1.0.6 版本。

有关变更和问题修复的完整列表，请参阅"Windows 开始菜单"下 SecurityGateway 程序组中的发布说明。

版本 9.5 的新功能

特殊说明事项

- 请在升级后审核 DNSBL[134] 和 URIBL[137] 列表和分值；已对这两个功能做出大量变化来支持新增的功能。
- 将出现的所有“白名单”和“黑名单”分别重命名为“允许列表[33]”和“阻止列表[35]”。
- 已删除通过 Vouch by Reference (VBR) 的邮件证书这一功能。因为没有已知的处于活动状态的证书供应商。该标准未被广泛使用，很遗憾它已经名存实亡了。

新功能

MDaemon (XML API) 用户验证源[55]

MDaemon (XML API) 已被添加为用户验证源[52]的新类型。MDaemon 的 XML API 为 Minger 提供了更好的替代方案，因为它可以使用可逆加密对 MDaemon 未存储密码副本的账户进行身份验证。它还能在一次调用中返回账户的所有别名。**注意：**该选项需要 MDaemon 23.0.2 或更高版本。

用于无密码登录和双重验证的 WebAuthn 支持[60]

SecurityGateway 现在可以允许用户使用 Web Authentication API (也称为 WebAuthn)进行登录，该 API 允许用户使用生物识别技术、USB 安全密钥、蓝牙等进行身份验证，从而为用户提供安全、无密码的登录体验，那么请选中此框。它也能被用作“双重验证”的额外验证方式。可以从用户选项[60]页面启用或禁用 WebAuthn 支持。用户可以在我的账户 » 设置[33]页面上注册其无密码登录凭证，可以在我的账户 » 双重验证[29]页面上注册其“双重验证”设备。还请参阅：webauthn.guide 来获取有关 WebAuthn 如何运作的更多详细信息。

Spamhaus 数据查询服务 (DQS)[145]

新增对于“数据查询服务 (DQS)”的支持，它是一套 DNSBL[134]，它们实时进行更新并由 Spamhaus Technology 运营，以便阻止超过 99% 的由电子邮件带来的威胁。DQS 需要由 Spamhaus Technology 提供的有效订阅和使用密钥。

其他功能和变更

- 在各自的页面上新增将邮件日志、用户隔离、管理隔离和邮件队列列表导出到 CSV 文件的选项。
- 邮件投递[74]页面现在拥有选项，以便在为暂时或永久的投递失败发送未投递报告 (NDR) 时，“*..包含用于通知发件人的完整邮件记录*”。默认情况下禁用这些选项；仅会包含来自远程 SMTP 服务器的最终错误消息。
- 新增功能来更改 DNSBL[134] 和 URIBL[137] 顺序。列表顶部的条目是查询的第一个条目。
- 邮件投递[74]页面现在有一个选项，用来管理 SMTP 连接故障和 SMTP 主机故障缓存。可以启用/禁用这些缓存，并且可以指定条目保留在缓存中的时间。
- 已为爆发保护[126]添加 HTTPS 支持。
- 新增指向“管理隔离报告”电子邮件模板的链接，以从管理隔离中删除个别邮件。

- 已在隔离配置 71 页面上新增选项，以便不在用户隔离报告邮件中包含 "始终允许"这个链接。

有关变更和问题修复的完整列表，请参阅 "Windows 开始菜单"下 SecurityGateway 程序组中的发布说明。

9.0.2 版本的新功能

特殊说明事项

- 9.0.3 — 爆发保护 126 已在 SecurityGateway 中恢复使用。
- 9.0.2 — Cyren Anti-Virus 已被 IKARUS Anti-Virus 取代。我们的安全技术合作伙伴之一 Cyren 最近宣布对公司及其产品进行快速清算。这就需要我们找到一个新的反病毒合作伙伴。经过彻底的评估，IKARUS Anti-Virus 以其出色的检测率和速度脱颖而出。它提供了可靠的保护，防止恶意和潜在的敌对程序，并将传统的防病毒防御措施与最新的前瞻式技术相结合。IKARUS Anti-Virus 每 10 分钟自动更新其定义。
- 9.0.0 — 默认情况下，包含加号(+)的邮箱名称现在将被视为子寻址 64 。用户验证进程将会将子寻址视为别名。例如，user+folder@example.com 将被解析成 user@example.com 和一个别名，其中 user+folder@example.com = user@example.com。无法创建其邮箱名称包含加号的新用户。邮箱名称包含加号的现有用户不会被自动删除。可以通过在用户验证源 52 页面上运行 "验证用户"进程来修复它们。新增一个用来恢复之前行为的选项（名为 *"允许用户邮箱名包好加号(+)字符"*）位于用户选项 60 页面上。启用后，这些邮箱名称将不会被视为别名/子寻址。例如，user+folder@example.com 将被视为其自己的用户，而不是 user@example.com 的别名。

主要新功能

发件人报头屏蔽 171

新的发件人报头屏蔽 171 页面被添加到反欺诈 148 部分，位于安全 124 下，它有助于揭露垃圾邮件发送者发送的邮件中存在欺骗性的 "发件人"报头，这可能诱使用户相信邮件是从合法来源发送的。

已增强网络界面的实用性

- 已将 "搜索"对话框更改成使用 *"显示/隐藏搜索"*工具，并在主工具栏中新增一个 *"取消搜索"*按钮。
- 新增 4 个额外的搜索报头模式，其中 "结果"和 "原因"位于邮件 254 页面上。可以使用按钮切换，由 AND/OR 来分隔报头模式。"结果"和 "原因"始终由 OR 分隔。
- 目前在域列表 41 和用户列表 48 的工具栏上有一个基本的搜索选项。
- 您现在可以调整大小，移动或最大化弹出窗口。
- 新增对移动端很友好的列表编辑器。
- 已将 "上一个/下一个"按钮添加到已归档邮件视图中。
- 已将 "已恢复邮件"这种状态邮件添加到搜索归档 88 页面的右下角。

已改进管理仪表板页面

- 当前，在仪表板[9]页面上向全局管理员显示可用磁盘空间，位于“设置/用户 » 系统”下的磁盘空间[110]页面上。
- 处于活动状态的 SMTP 入站和出站会话已被添加到仪表板上。
- 已将管理和用户隔离队列中的邮件计数添加到面向全局管理员的仪表板页面。
- 您现在可以从“仪表板”冻结入站和远程投递队列。

其他功能和变更

- 当前“设置 » 系统 » HTTP 服务器”页面有一些选项，用来将 HTTP Strict Transport Security (HSTS) 报头[107]包含在 HTTPS 响应中。默认情况下，启用该选项。当支持 HSTS 的浏览器收到 HSTS 报头，并且 SSL 证书有效时，以后对同一域发出的任何 HTTP 请求将自动升级为 HTTPS。
- SecurityGateway 现在支持较新的 Windows 版本中的 TLS 1.3。Windows Server 2022 和 Windows 11 默认启用 TLS 1.3。Windows 10 版本 2004（OS 版本 19041）和更高版本具有实验性的 TLS 1.3 支持，可以通过在注册表中设置以下内容来启用入站连接：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityP
  roviders\SCHANNEL\Protocols\TLS 1.3\Server

DisabledByDefault (DWORD) = 0

Enabled (DWORD) = 1
```

- 新增一个选项，允许用户查看隔离报告中列出的邮件。全局管理员可以在：设置/用户 » 邮件配置 » 隔离配置[71]或主页 » 我的账户 » 设置[31]中启用它。
- 只要“记住我[60]”选项在当前设备或浏览器上处于活动状态，在用户的我的账户 » 设置[31]页面上就提供*“在该设备/浏览器上不记住我”*这个选项。他们可以点击该链接来停用该设备上的“记住我”状态，然后该链接将消失。在他们下次登录 SecurityGateway 时，他们仍然能够使用*“在该设备上记住我”*这个选项。在“记住我”当前处于活动状态时，也向安全通信[92]用户提供该选项。
- 在账户 » 用户选项[60]和安全通信 » 收件人选项[92]页面上提供新选项，允许您分别在 SecurityGateway 的登录页面和 Secure Messaging 登录页面上添加一些管理员联系信息。
- 已在用户验证源编辑器[55]中新增“保存和测试”按钮。
- 已在登录页面新增 CSRF 令牌，并向 web 界面 URL 添加了辅助会话 ID，以缓解 CSRF 攻击。
- 新增公共/私人密钥验证方式，作为记住我[60]功能的一部分。
- 已使用新样式和略有不同的语言更新了安全消息通知电子邮件。
- 已减少数据库事务处理数量。这有助于防止数据库变大。
- 已在归档 » 合规[89]页面新增一个选项，由此来*“仅删除活动的归档储库中的邮件”*。该选项控制是否将删除非活动归档储库中的较旧的已归档邮件，以及活动的储库中的旧归档邮件。默认情况下启用此选项，这意味着只会删除活动储库中的旧邮件。此行为与以前的版本保持不变。
- 现在如果在 IP 阶段，SIEVE 行为发生“错误”或“拒收”，则断开 SMTP 套接字连接。

- 在启动时，现在已将入站队列中被锁定的邮件移动到"CrashDumps\InboundQueue"目录。当向发件人发送响应时，将解锁入站队列中的邮件。如果 SecurityGateway 进程崩溃或在有机会关闭之前终止，则被锁定的邮件可能会在入站队列中成为孤立邮件。由于发件人没有收到针对 SMTP DATA 命令的响应，他们应该再次发送邮件。投递该邮件可能导致收件人接收多个副本。不过，这些邮件的内容可能有助于调试崩溃。任何移到此目录的邮件将在30天后被自动删除。
- LetsEncrypt[104] - 已更改"日志"功能来使用 add-content 而不是 out-file。Add-content 使用默认的系统代码页面，应该能使用户在 SecurityGateway 中查看日志文件。在创建新的日志文件之前，不会对日志文件的编码进行任何更改。

有关变更和问题修复的完整列表，请参阅"Windows 开始菜单"下 SecurityGateway 程序组中的发布说明。

8.5.0 版本的新功能

特殊说明事项

已弃用 32 位版本并停止对 32 位操作系统的支持。从 SecurityGateway 8.5.0 开始，只提供 64 位版本。这使我们能够简化开发和测试，并使用仅适用于 64 位的库。如果您当前正在我们支持的 64 位操作系统上运行 32 位版本，您只需下载 64 位版本，并覆盖安装即可。

主要新功能

安全通信网络门户[90]

SecurityGateway 新的"安全通信"功能为您的用户提供了一种向其域外的收件人发送安全邮件的方式，通过这种方式，邮件绝不会离开 SecurityGateway 服务器。它通过使用安全的通信网络门户来实现这一点。发送邮件后，收件人会收到一封电子邮件通知，告知他们有可用的安全邮件，其中包含用于创建安全邮件收件人[91]账户的链接，以便他们可以查看位于您 SecurityGateway 服务器上的邮件。通过收件人的浏览器访问安全邮件，并通过 HTTPS 加密在 SecurityGateway 服务器和收件人之间维护端到端的加密。安全通信需要有效的 SSL 证书[103]并启用 HTTPS[100]（还请参阅：HTTPS 服务器[107]）。收件人可以查看和答复 SecurityGateway 门户中的邮件，并且他们可以选择性地向指定的用户列表编写新的安全邮件[95]。还请参阅：收件人[91]和收件人选项[92]来获取有关安全邮件收件人账户的更多信息。

基于用户的邮件路由

- 借助用户编辑[48]页面上新的"邮件投递"部分，您可以为用户的邮件选择特定的域邮件服务器，而不是使用分配给域的默认邮件服务器。
- 已将一个新选项添加到"域属性[43]"对话框：*"不使用此邮件服务器投递域邮件，仅可将其分配给特定的域用户"*。
- 这些设置允许异构式部署，其中一些本地用户的邮箱托管在云中，而其他用户则位于本地。这也使您可以使用单个域和单个 SecurityGateway 服务器，将邮件路由到在您企业的每个位置运行的邮件服务器。

性能计数器 269

SecurityGateway 现在还提供各种 "性能计数器"，供 "Windows 性能监控器"使用，使您可以实时监控 SecurityGateway 的状态。提供许多计数器，例如活动的入站和出站 SMTP 会话数、排队等待投递的邮件数、隔离的邮件数、SecurityGateway 已运行多长时间、域和用户计数等。

其他功能和变更

- 已在 "用户选项 60"页面上新增一个选项来要求强密码。可以在 "用户编辑 48"页面上按用户禁用此项。
- 如果使用服务提供商/私有云注册密钥，现在将显示仪表盘和注册页面。
- 用于附件过滤的收件人允许列表 203。新增针对附件过滤的收件人允许列表。用户能为绕过相关过滤的附件阻止和隔离定义收件人地址列表，支持通配符。
- Lets Encrypt - 该脚本将不会在每次运行时删除日志文件。

有关变更和问题修复的完整列表，请参阅 "Windows 开始菜单"下 SecurityGateway 程序组中的发布说明。

版本 8.0.0 新功能

主要新功能

- SecurityGateway 现在支持您集群 111环境中的 active/active 数据库复制，但它需要外部的复制工具，其配置超出了本帮助文件的范围。有关如何配置集群来使用 active/active 复制的要求和指南，请参阅 PDF 文档：SecurityGateway: Configuring Active-Active Database Replication。
- 数据泄露防护 - 搜索医学术语 193。可以定义医学术语列表，并为每个术语分配分数。扫描邮件来查找匹配的术语，并计算找到的所有术语的分数总和。对计算的分数超过定义阈值的邮件，执行指定的操作。
- 添加了在邮件处理期间，运行自定义进程/脚本，并根据脚本结果选择操作的功能。
  - 该脚本必须放在 "Sieve Executable Path"目录中，可以从 "设置 » 系统 » 目录 109"进行配置。
  - 已新增 "execute 230"这个 sieve 关键字，可以用作操作和测试。
  - 第一个参数是脚本的名称。现在支持 .bat、.exe 和 PowerShell。
  - 第二个参数是将传递给进程的参数。"message_filename"这个 sieve 变量填充了当前正在处理的邮件的 RFC822 源的完整路径。
  - 例如 ... if execute "Test.ps1" "-msg '${message_filename}'" {}
- 新增为域导出所有已归档邮件 90的功能。
- 变更/审计日志 261 - 新增一个新的日志文件，其中记录了对配置的变更以及更改者。
- 新增按照定义的调度将隔离报告 71发送给用户和管理员的功能。

- 为通过邮件发送的隔离报告ÐÂÔöÒöÑìÏî[71]，以便仅包括自上次发送隔离报告电子邮件以来已被隔离的新邮件。如果隔离报告中没有要包含的新邮件，则不会生成隔离报告。

其他功能和变更

- 已更新 "忘记密码[60]"进程来发送含有链接的邮件，以便更改用户的密码。
- LetsEncrypt[100] - 已更新脚本来查找由 LetsEncrypt 使用的新颁发者。
- 已更新 DKIM 签名[155]来使用 SHA256 Hash。
- 已为 XMLRPC API 和 PowerShell 模块新增 GetServerSetting 和 PutServerSetting 方式。
- 已为 "设置 » 邮件配置 » 邮件协议[76]"页面新增 SMTP 连接和协议超时。
- 新增从 "邮件日志[260]» 邮件信息 » 邮件"选项卡下载附件的功能。
- 已更新警报、确认和提示消息框。
- 在 docs\API\PowerShellSamples 目录中添加了几个 PowerShell 脚本示例，以供参考。
- 现在，HELO 域名[76]值（"设置 » 邮件配置 » 邮件协议）是 集群环境中按服务器的设置。可以将该值设置为集群中每个服务器上的唯一值。
- 新增对照 web 界面的数据库，手动执行 SQL 语句[120]的功能。此功能只能在技术支持的指导下使用，建议先进行数据库备份。
- 新增选项来将 "将域列入阻止列表"这个链接包含于隔离报告邮件[71]中。

有关变更和问题修复的完整列表，请参阅 "Windows 开始菜单"下 SecurityGateway 程序组中的发布说明。

版本 7.0.0 新功能

特殊说明事项

- 在邮件协议[76]页面上（位于 "设置 » 邮件配置 » 邮件协议），删除了两个选项：*尽可能使用 ESMTP* 和 *隐藏 ESMTP SIZE 命令参数*。现在，这两个选项将很显眼，并尽可能使用 ESMTP。
- 因为已改变并弃用 clamd.conf 中的许多设置，现在安装程序将覆盖现有的 clamd.conf。如果您已定制了 clamd.conf，您可能需要在安装后审核和更改它。
- 已删除日志配置[262]选项，用来 *"基于星期几创建日志文件"*。如果选中此项，升级进程会将其更改成 *"每天创建一套新的日志文件"*。

新功能和变更

集群 111

SecurityGateway 新的集群功能的设计旨在：在网络上的两个或多个 SecurityGateway 服务器之间共享您的配置。这使您可以使用负载均衡硬件或软件，在多个 SecurityGateway 服务器之间分配电子邮件负载，从而可以通过减少网络拥塞和过载，并最大化电子邮件资源来提高速度和效率。如果一台服务器发生硬件或软件故障，该功能还有助于确保电子邮件系统中的冗余。以下是有关 SecurityGateway 集群功能的许多要点（有关更多详细信息和设置说明，请参阅：集群 111）：

- 集群允许多个处于活动状态的 SecurityGateway 实例/服务器共享一个数据库。
- 必须手动安装和配置外部的 Firebird 版本3数据库服务器。
- 安装程序中已添加一个选项，允许在初始安装期间指定外部的 Firebird 服务器参数。可以将现有的安装配置为通过 sgdbtool.exe 命令行工具连接到外部的 Firebird 数据库服务器。
- 需要共享存储，并且共享目录必须设置为集群中所有服务器都可以访问的 UNC 路径。这可能需要为 SecurityGateway Windows 服务 115更改用户账户。
- 主服务器负责调度的维护任务。
- 集群中的每个服务器必须具有自己的唯一注册密钥。

Firebird 3 数据库升级 112

- Firebird 2 和 3 运行时已包含并安装在 SecurityGateway 7.0 中。
- SecurityGateway 7.0 或更高版本的新安装将使用 Firebird 3。
- 将现有的 SecurityGateway 安装更新到 SecurityGateway 7 版本或更高版本时，将继续使用 Firebird 2。
- 使用新的集群 111功能需要 Firebird 3 数据库。
- 升级数据库以使其与 Firebird 3 兼容，要求使用 2.x 运行时进行备份，并使用 3.x 运行时进行还原。管理员可以使用 sgdbtool.exe 命令行工具（位于 \SecurityGateway\App 文件夹）来将现有的数据库从 2 版本升级到 3 版本。要转换数据库，请停止 SecurityGateway 服务，打开命令提示符，然后运行："**sgdbtool.exe convertfb3**"。

双重验证 60

在“用户选项 60”下，管理员可以全局或按域允许并要求双重验证（2FA）。如果需要 2FA，则首次登录时会向用户显示“设置 2FA”页面。否则用户可以前往“主页 » 我的账户 » 双重验证 29”来设置 2FA。

检查泄露的密码 63

SecurityGateway 可以对照来自第三方服务的已泄露密码列表来检查用户的密码，并且无需将密码传输到该服务即可执行此操作。如果用户的密码出现在列表中，并不表示该账户已被黑客入侵。而是意味着某人在某处使用了与他们的密码相同的字符，并且发生了数据

泄露事件。从未在其他任何位置使用过的唯一密码更加安全，因为黑客在字典攻击中可能会使用已公开的密码。请参阅 Pwned Passwords (已泄露密码)获取更多信息。

域管理员可以创建新域 51

这是 "编辑管理员 51"页面上的新选项，允许您授予域管理员创建新域的权限。管理员将被自动添加为他或她创建的任何域的 "域管理员"。还有一个选项可以设置允许管理员创建的域数限制。

新的 SMTP 扩展 100

RequireTLS (RFC 8689) 101

IETF 中的 RequireTLS 工作终于完成，并且已经实现了对此的支持。RequireTLS 允许您标记*必须*使用 TLS 的邮件。如果无法使用 TLS (或者 TLS 证书交换的参数不可接受)，则退回邮件，而不是不安全地投递邮件。默认情况下，启用 RequireTLS，但是将受 RequireTLS 进程约束的唯一邮件是被使用新的内容过滤器操作 199 "*为 REQUIRETLS 标记邮件...*"的 "内容过滤器"规则特别标记的邮件，或发送至<local-part>+requiretls@domain.tld (例如，arvel+requiretls@mdaemon.com)的邮件。将所有其他邮件视为已禁用该服务。此外，必须满足几个要求才能使用 RequireTLS 发送邮件。如果它们中的任何一个失败，该邮件将弹回，而不是以明文形式发送。有关这些要求以及如何设置 RequireTLS 的更多信息，请参阅启用 REQUIRETLS (RFC 8689) 101 选项。有关 RequireTLS 的完整说明，请参阅：RFC 8689: SMTP Require TLS Option.

SMTP MTA-STS (RFC 8461)-严格传输安全 102

IETF 中的 MTA-STS 工作完成了，并且已经实现了对此的支持。SMTP MTA 严格传输安全 (MTA-STS)是一种机制，使邮件服务供应商 (SP)能够声明其接收传输层安全 (TLS)和保护 SMTP 连接的能力，并指定发件 SMTP 服务器是否应拒绝投递给不为 TLS 提供受信任的服务器证书的 MX 主机。默认启用 MTA-STS 支持。请参阅启用 MTA-STS (RFC 8461) 102 选项来获取有关设置的更多信息。SMTP MTA-STA 的完整描述请参阅 RFC 8461: SMTP MTA Strict Transport Security (MTA-STS).

SMTP TLS 报告 (RFC 8460) 102

TLS 报告功能允许使用 MTA-STS 的域收到有关检索 MTA-STS 策略或使用 STARTTLS 协商安全通道的任何失败的通知。启用后，SecurityGateway 会每天向已在当天向其发送 (或尝试发送)邮件的每个启用 STS 的域发送报告。提供了多个选项来配置报告将包含的信息。默认情况下禁用 TLS 报告功能，更多详细信息请参阅RFC 8460: SMTP TLS Reporting.

其他功能和变更

- 已使用更现代的外观更新了 SecurityGateway GUI。
- 已更新 FusionCharts 图形组件。
- 新增功能来从病毒扫描 146 排除特定的发件人。
- 新增选项来使允许列表优于阻止列表 211。
- 现在，LetsEncrypt 将检查计算机上运行的 PowerShell 的版本，如果尚未安装正确的版本，则返回错误。
- LetsEncrypt 将检查 PSModulePath 环境变量，以确保包括了 SG 模块路径，如果不包含，则会为会话添加该路径。

- 当在暂存和实时 LetsEncrypt 系统之间进行切换时，LetsEncrypt 将删除并重新创建账户。
- 当挑战失败时，LetsEncrypt 将从 LetsEncrypt 检索错误，并将数据写入日志和屏幕。
- LetsEncrypt 有一个新的 -Staging 参数，可以在命令行上传递它。如果通过了此参数，脚本将使用 LetsEncrypt 暂存系统请求证书。
- 已将 JSTree 库更新到 3.3.8 版本。
- 新增功能来指定 SecurityGateway Windows 服务115在哪个用户账户下运行。
- 新增 SIEVE 变量扩展 RFC-5229 支持。
- 在 "SIEVE 变量扩展"中添加了：eval修饰符，帮助您进行简单的计算。

  示例：

```
require "securitygateway";
require "variables";
require "fileinto";

if header :matches "from" "*" {
    set :length "length" "${1}";
    set :eval "fileintovar" "${length} * 25 - 1 / 8+3";
    fileinto "${fileintovar}";
}
```

- 已删除 "基于星期几创建日志文件"这个选项。如果选中此项，升级进程会将其更改成 "每天创建一套新的日志文件262"。
- 新增一个选项，可以在输入密码时切换密码查看。在用户选项60页面上新增一个访问控制选项，允许禁用此功能。
- 在下载病毒定义时，将 Cyren AV 更新程序更改为使用 TLS。
- 新增选项以在日志文件名中包含计算机名262。如果日志目录被设置成 UNC 路径，则此项为必要选项，而且它允许一个集群中的多个服务器记录到同一个位置。
- 已向安装程序新增选项，以在初始安装期间指定外部的 Firebird 服务器参数。
- 已将 Chilkat 库更新为 9.5.0.82 版本。
- 新增一个日志选项262，用于不记录来自指定 IP 地址的 SMTP 或 HTTP 连接。来自指定 IP 地址的不完整和拒绝的 SMTP 邮件也不会添加到数据库中。如果邮件被接受进而投递，它将被添加到数据库中。
- 新增 Sieve 操作 "changesender"，以允许 SG 用来发送/更改邮件的 SMTP 信封发件人。
- 已将 Cyren AV 引擎更新到 6.3.0r2 版本。
- 已将 ClamAV 引擎更新到 0.102.4 版本。

有关变更和问题修复的完整列表，请参阅 "Windows 开始菜单"下 SecurityGateway 程序组中的发布说明。

章节

2

2 主页

2.1 仪表板

您登录 SecurityGateway for Email Servers的第一个页面是 "仪表板"，位于主页菜单下方。该仪表板可以让您快速地概览 SecurityGateway 的当前状态与一些关于其近 24 小时内活动的摘要报告[266]。

仪表板顶部是*服务器状态*部分。该部分告诉您 SMTP 会话是否运行，并提供您可以启动或停止会话的链接。此外，控制面板列出了您的注册码大小，提供链接来管理您的注册[121]与激活，并列出了当前存在的域与用户数。它还提供了通往域列表[41]的链接以管理您的域和用户。在软件更新[120]可用时，本节还将提供有关更新的详细信息的链接。然后，将显示 SMTP 入站和出站会话的活动会话数，并且 "队列状态"部分将列出入站、投递和坏邮件队列中的邮件数。在同一部分中，对于全局管理员，还列出了 "管理员和用户隔离"中的邮件数。此外，在 "入站和投递队列"的条目中，有一个选项可以冻结/解冻每个队列。在*服务器性能*部分中，"全局管理员"可以查看 "可用磁盘空间"总量。然后，将显示系统和 SecurityGateway 的 CPU、物理内存和虚拟内存统计信息、IKARUS[146]、ClamAV[146] 和 SpamAssassin[129] (SpamD[131]) 进程。

"服务器状态"部分下是*"服务器统计"*部分。该部分显示了 SecurityGateway 的六个图表报告：接收 vs. 外发邮件[266]，邮件占用的总带宽[266]，合法 vs. 垃圾邮件[266]，垃圾邮件分析[266]，顶级邮件收件人[267]，与顶级垃圾邮件域[268]。每个报表都显示了近 24 小时内的统计数据。如果您希望更改要显示的报告，或创建新报告和自定义报告进行显示，请点击**自定义图表**。最后，报告和自定义图表具有元素，您可以将指针悬停在这些元素上，来查看有关这些元素的详细信息。对于自定义图表，您还可以通过单击图表数据点向下挖掘关联的邮件日志条目。

域管理员[50]将只能看到他们具有管理权限的域的统计信息和选项。

2.2 我的账户

当您登录到您的 SecurityGateway 用户账户时，看到的第一个页面就是 "我的账户登录页面"。它包含两部分：账户设置和账户统计 账户设置部分包含指向你希望执行的常规任务的链接。点击任何一个链接将跳转到与该任务有关的页面。该账户统计 分显示了在过去 24 小时内与您的账户活动相关的四份报告。*良好 vs. 垃圾邮件*报告显示了已为您的账户处理好的良好邮件较之垃圾邮件的总数。垃圾邮件就是那些被识别为垃圾邮件、诈骗，包含病毒一类的邮件。*"垃圾邮件分析"*根据类型分类显示收到的所有垃圾邮件总数。*"入站 vs. 出站邮件"*显示您接收的入站邮件总数和您发送的出站邮件总数。*"垃圾邮件来源排行"*显示了最频繁向您发送垃圾邮件的发件人。

左侧导航窗格中的 "主页"标题下，有若干与您用户账户相关的链接：

我的账户

- **登录页面**——将您带入 "我的账户登录页面"，其中列出了一些与账户相关的常见任务的链接。

- 双重验证[29]—当您使用安全连接（即在浏览器中用于访问 SecurityGateway 的地址中使用 "https://"登录）时，"双重身份验证"页面将显示在"我的账户"选项下。"双重验证"有助于使您的账户更安全，除了输入您的常规电子邮件地址和密码以外，还要求您输入验证代码、在设备上使用指纹进行身份验证，或者在登录 SecurityGateway 时使用其他其他验证方法。**请注意：**即使使用安全连接，某些用户也可能无法使用"双重身份验证"。
- 设置[31]——该链接将您带入您的"账户设置"页面，该页面用于更改您的密码，设置您的隔离区首选项，打开自动允许列表，以及指定您希望显示在页面上的条目数。
- 允许列表[33]—点击此链接来查看您的个人地址允许列表。向您的允许列表添加地址，有助于防止 SecurityGateway 将发件人的邮件错误地识别为垃圾邮件或者完全阻止它们。
- 阻止列表[35]—该链接会将您带往个人地址阻止列表。当您不希望从某个地址收到更多邮件，将该地址添加至您的阻止列表。

- 查看我的隔离区[37]——当 SecurityGateway 收到那些看起来非常可疑而无法投递给您的邮件时，它们会被存储在您的隔离文件夹中。您可以从该页查看被隔离的邮件，解除它们的隔离状态（意味着这些邮件是应该投递给您的合法邮件），删除邮件，或者将其发件人添加至您的允许列表[33]或者阻止列表[35]。
- 查看我的邮件日志[38]——点击该链接以查看所有您已发送或已接收的邮件的日志。您可以使用此日志来查看每封邮件的详细信息，将邮件标记为垃圾邮件或非垃圾邮件，并将地址列入允许列表或阻止列表。

您可能无法使用一些选项，这取决于 SecurityGateway 赋予您账号的访问等级。

2.2.1 双重验证

当您使用安全连接（即，在浏览器中用于访问 SecurityGateway 的地址中使用 "https://"登录）时，"双重身份验证"页面将显示在"我的账户"选项下。"双重验证"（即两步验证）有助于使您的账户更安全，除了输入您的常规电子邮件地址和密码以外，还要求您输入验证代码、在设备上使用指纹进行身份验证，或者在登录 SecurityGateway 时使用其他其他验证方法。例如，在使用 Google Authenticator 应用程序时，验证码会不断改变，并在登录时从手机或设备上安装的应用程序中获取。这意味着即使有人设法获取您的 Webmail 密码，他们仍然无法登录到您的 Webmail 账户，因为他们将无法获得验证码。

即使使用安全连接，某些用户也可能无法使用"双重身份验证"。

设置"双重验证"

遵照下方指示来设置您希望使用哪种"双重验证"方式。在您设置一个以上的方式时，您可以选择在登录时希望使用哪一种方式。

使用设备验证

要设置设备验证，例如使用 USB 安全密钥、或者您手机或笔记本电脑上的指纹识别器等：

1. 请在浏览器中使用 "https://"而不是 "http://"来登录 SecurityGateway。
2. 在 "我的账户 » 双重验证"下方，请点击 **"设置设备验证"**。
3. 在 "设备验证设置"框中，请选择您希望使用的设备类型。
4. 输入您的 **"当前密码"**并点击 **"开始"**。
5. 请按照指示选择并验证您的设备。
6. 完成时，将在 "设备验证"框中显示一个条目。

验证器应用程序

要使用 Google Authenticator 应用程序来设置 "双重验证"：

1. 在您的手机或设备上安装 Google Authenticator 应用程序或兼容 Google Authenticator 的应用程序。
2. 请在浏览器中使用 "https://"而不是 "http://"来登录 SecurityGateway。
3. 转至 "我的账户 » 双重验证"页面，并输入您的 **"当前密码"**。
4. 在 "验证器应用程序设置"下方，请点击 **"设置验证器应用程序"**。
5. 在您的验证程序中，请依次选择 **"设置账户"**、**"扫描二维码"**并扫描页面上的二维码。
6. 如果您无法扫描二维码，请点击 **"显示密钥"**并在程序中输入密码和您的邮件地址。
7. 在您的应用程序中输入 "验证码"并点击 **"验证配对"**。

使用电子邮件验证

要设置接收验证码的辅助电子邮件地址 (电子邮件代码通常在 10 分钟后过期)：

1. 请在浏览器中使用 "https://"而不是 "http://"来登录 SecurityGateway。
2. 转至 "我的账户 » 双重验证"页面，并输入您的 **"当前密码"**。
3. 在 "电子邮件验证"下方，输入 **"验证码电子邮件"**地址。
4. 在 **"确认验证码电子邮件"**下方，再次输入相同的地址。
5. 点击 **"设置电子邮件验证"**。
6. 会将一封包含验证码的电子邮件发送至您提供的电子邮件地址中。请输入验证码并点击 **"验证电子邮件"**。

禁用双重验证

要禁用 "双重验证"，请在 "双重验证"页面上输入您的 **"当前密码"**并在您希望禁用的方式下，使用 **"撤销"**或 **"禁用双重验证"**选项。

2.2.2 设置

"账户设置"页面用于更改您的密码、设置隔离首选项、启用自动列入允许列表、并指定您希望显示在页面上的条目数。

您可能无法使用一些选项，这取决于 SecurityGateway 赋予您账号的访问等级。

更改密码

密码
要更改您的密码，请在此处输入新密码。

密码（确认）
在以上的密码框中输入了您的新密码之后，在此处再此输入密码以进行确认，接着请点击*"保存"*。

隔离

为我的域使用默认的隔离设置
这是通常会选择的选项。选择该选项以让您的隔离 37 选项按照您邮件管理员的原始设置进行设置。

允许我指定我自己的隔离设置
如果您希望修改您的隔离设置请选中该选项，并选择以下您想要的选项。

在服务器上保留被隔离的邮件
如果您选中该选项，SecurityGateway 会将非常可疑的接收邮件保留在隔离区 37，让您稍后对它们进行检查。

发送列出我隔离文件夹内容的邮件：
如果您已经选择让 SecurityGateway 隔离可疑的邮件，您还可以选择让其定期发送您一封邮件，该邮件列出了您隔离文件夹中的当前内容。

从不
如果您不希望收到这封邮件，它会列出您被隔离的邮件，请选中该选项。

每 [xx] 小时
如果您希望每隔某几个小时就收到这封邮件，请选中该选项并指定想要的值。

每天
这是通常会选择的选项。这会让 SecurityGateway 每日发送您一封邮件，它会列出您被隔离的邮件。

每周
如果您希望每周都能收到此邮件一次，请选中该选项。

按以下值排序隔离邮件：[已接收 |发件人 |主题]
使用此选项可选择您希望如何对隔离电子邮件中包含的隔离邮件列表进行排序。默认情况下，列表按收到邮件的日期排序，但您也可以选择按发件人或主题排序。

在隔离列表和邮件中包含 "列入阻止列表"选项
选中此项后，您的隔离邮件列表和隔离报告电子邮件中将提供一个链接，该链接可供您用于将发件人的电子邮件地址添加到阻止列表中。

在隔离列表和邮件中包含 "将域列入阻止列表"选项
选中此项后，您的隔离邮件列表和隔离报告电子邮件中将提供一个链接，该链接可供您用于将发件人的域添加到阻止列表中。

I在隔离邮件中包含 "查看邮件"选项
如果您希望在隔离报告电子邮件中包含 "查看邮件"这个选项，请选中此框，以允许您查看隔离邮件。

允许我的邮件服务器或者客户端过滤被隔离的邮件
如果您不希望 SecurityGateway 隔离任何您接收的邮件，请选中该选项。本来要被隔离的邮件就会照常投递。如果您希望您的邮件服务器或者邮件客户端过滤您的邮件，这会很有帮助。为了帮助您识别本来要被隔离的邮件，您可以使用以下的两个选项来为邮件主题添加标签或者向邮件添加一个特殊的报头。之后您可以创建一个过滤器或在您的服务器或邮件客户端中进行管理以搜索那个标签或报头。

...用 [文本]标记主题
当您选中该复选框，SecurityGateway 会将某些文本添加至邮件主题，那些邮件是在您打开隔离选项时将被隔离的邮件。默认情况下，该选项提供的文本是："*** SPAM ***"(*** 垃圾邮件 ***")。但是，您可以根据自己的需求更改该文本。

...添加报头 [文本]
当选中该复选框，将为本来要被 SecurityGateway 隔离的任何邮件添加特殊的报头。在大多数的邮件客户端中，如果不查看邮件的属性或来源，您将无法看见报头，但是在许多邮件客户端与邮件服务器中，您可以创建过滤器来寻找那个报头并对具有该报头的邮件进行一系列特定的处理，比如将那些邮件置于指定的文件夹或者删除它们。该选项为您提供的报头是："X-Spam-Flag: (X-垃圾邮件-标记：) YES (是)"。但是您可以按照自己的选择对报头进行更改。

选项

不为该账户归档邮件
如果您不希望存档此账户的邮件，请选中此框，即使此账户所属的域设置为存档邮件也是如此。此项仅适用于管理员

为此账户删除所有已归档的邮件
如果您希望删除此用户收发的**所有**归档邮件，请点击此项。系统将要求您确认删除所有已归档邮件的决定。

将接收我所发邮件的地址自动列入允许列表
当选中该复选框，任何您发送邮件的地址都会被自动地添加到允许列表[33]。这有助于确保 SecurityGateway 在未来不会将来自那些地址的邮件错误地识别为垃圾邮件或阻止它们。

对发往该账户的邮件不执行反垃圾邮件测试
如果您不希望服务器对邮件地址是您帐户的邮件执行反垃圾邮件测试，请选中该复选框。这将阻止执行各种反垃圾邮件测试，并且极大地增加了您账户将会收到的垃圾邮件的数量。

使该账户免于"账户劫持检测"
如果您希望免于账户劫持检测功能，请启用此选项。在短时间内合法发送大量邮件的账户可能需要豁免。

何时显示统计图表
使用此选项可以选择何时将统计图显示在仪表盘和登录页面[28]上。您可以选择自动、始终、手动或从不。

语言
使用此下拉式列表来设置服务器发送系统信息时使用的语言。

每页显示的项目数
该选项决定了在您登录 SecurityGateway 时，每页将显示的条目数量，例如您允许列表中的地址，您邮件日志中的条目等等。如果在单页上由于条目数太多而无法完全显示的时候，每页底部会出现一些控制按钮帮助您翻转至另一页。

在该设备/浏览器上不记住我
如果您在登录 SecurityGateway 时使用了*"在该设备上记住我"*这个选项，则会在此处显示该选项。如果您想为这个设备或浏览器取消"记住我"，您可以点击此链接。在您下次登录时，您仍然能够使用*"在该设备上记住我"*这个选项。

已注册凭证

该区域包含用于无密码登录的已注册凭证列表。要添加新的无密码登录凭证：

1. 请在浏览器中使用"https://"而不是"http://"来登录 SecurityGateway。
2. 在"我的账户 » 设置"页面的"已注册凭证"下方，请点击**"新建登录凭证"**。
3. 在"无密码登录设置"框中，请选择您希望使用的设备类型。
4. 输入您的**"当前密码"**并点击**"开始"**。
5. 请按照指示选择并验证您的设备。
6. 完成后，对于您刚才添加的凭证，**"已注册凭证"**框中将显示一个条目。

2.2.3 允许列表

允许列表是您的个人列表，其中列出已允许的地址。向您的允许列表添加地址，有助于防止 SecurityGateway 将发件人的邮件错误地识别为垃圾邮件或者完全阻止它们。通常您一次只可以将一条地址添加到该列表，但是您可以使用允许列表具有的导入功能，一次性将

包含在一个文本文件中的多条地址全部添加至黑名单。此外，您的允许列表还具有导出功能，可以将您允许列表的内容保存为一个值以逗号分隔 (CSV)的文本文件。

添加地址到允许列表

要将地址添加至您的允许列表，请单击位于该页顶部工具栏中的 *"新建"*。这会打开允许列表条目 35 页面用以添加地址 (如下)。

编辑允许列表地址

要编辑列入允许列表的地址，请双击想编辑的条目，或选择所需条目，然后在页面顶部工具栏上点击 *"编辑"*。这将会在允许列表条目 35 页面打开该条目。

删除列入允许列表的地址

要删除一条或多条列入允许列表的地址，请选择所需条目，然后在页面顶部工具栏上点击 *"删除"*。在点击每个条目的同时按下 CTRL 键可选择多个条目。点击 *"删除"*后，会弹出确认框，询问您是否确实要删除选定项。

将地址导入允许列表

要将地址导入到您的允许列表，请点击位于该页顶部工具栏中的 *"导入"*。这会打开导入列表页。使用位于该页的 *"浏览"*按钮来寻找文本文件，该文件包含了您希望导入的地址，然后请点击 *"导入列表"*。

该文本文件每行必须只能有一条地址，您应该使用标准的文本编辑器 (比如 Notepad)来创建它，以防在不经意间插入了任何不常见的格式或者字符，从而防碍了导入过程。

使用 CSV 文件导入

如果您希望为每一条被导入的地址添加对应的注释，那么在您导入这些地址的时候，您将需要使用 CSV 文件，而不是一个简单的地址列表。您可以使用任何纯文本编辑器，比如 Notepad 来创建 CSV 文件。只需按以下格式创建文件并保存为 *文件名.csv*。CSV 文件的第一行必须是映射行，以让 SecurityGateway 知道数据是按什么顺序出现的。文件中的每一项都必须包含在引号中，并以逗号分隔。

格式：

CSV 需要两列：*值*与*注释*。*"值"*列是用于您希望添加至允许列表的邮件地址，而 *"注释"*列是用于关于每个条目您希望添加的任何批注。该列表中任何没有注释的条目，同样需要引号，引号中无内容，以表示该条目没有注释。

CSV 文件内容示例：

```
"Value","Comments"("值","注释")
"myfriend@example.net","A comment about my friend."("关于我朋友的注释")
"someone@example.org",""
"mister@domain.com","A comment about mister."("关于我先生的注释")
```

从允许列表导出地址

要导出您的地址允许列表：

1. 在页面顶部工具栏上点击 *"导出"*。这会打开文件下载对话框。

2. 点击 *"保存"*。
3. 选择文件名称和位置。
4. 点击 *"保存"*，然后是 *"关闭"*。

允许列表条目

该页用于向允许列表中添加新地址和编辑现有条目。只要您点击位于该列表顶部工具栏中的 *"新建"*或 *"编辑"*，就会打开这个页面。

列表项

电子邮件地址：
在第一个框中，输入您希望添加至允许列表的邮件地址。您可以在地址的邮箱部分使用星号，以将该域的所有地址归入允许列表。例如，"*@example.org"把来自 example.org 的所有邮件列入允许列表。

注释：
在该区域可输入有关该条目的任意注释或说明，供自己参考。

保存与关闭
完成条目编辑后，点击 *"保存并关闭"*将该条目保存到允许列表中。

关闭
如果您希望关闭 "允许列表条目"页面且不作保存，请点击该按钮。

2.2.4 阻止列表

阻止列表是您的个人列表，其中列出已阻止的地址。如果您不希望将您的邮件发送至某些地址，您应该将这些地址添加至您的阻止列表。通常您一次只可以将一条地址添加到该列表，但是您可以使用阻止列表具有的导入功能，一次性将包含在一个文本文件中的多条地址全部添加至黑名单。此外，您的阻止列表还具有导出功能，可以将您阻止列表的内容保存为一个值以逗号分隔 (CSV)的文本文件。

添加地址到阻止列表

要将地址添加至您的阻止列表，请点击位于该页顶部工具栏中的 *"新建"*。这将打开阻止列表条目 36 页面，以添加地址 (见下)。

编辑被列入阻止列表的地址

要编辑一条列于阻止列表的地址，请双击您希望编辑的条目，或选中要编辑的条目并单击位于该页顶部工具栏中的*编辑*。这将会在阻止列表条目 36 页面打开该条目。

删除被列入阻止列表的地址

要删除一条或多条列于阻止列表的地址，选中要删除的条目并单击位于该页顶部工具栏中的 *"删除"*。在点击每个条目的同时按下 CTRL 键可选择多个条目。点击 *"删除"*后，会弹出确认框，询问您是否确实要删除选定项。

导入地址到阻止列表

要将地址导入到您的阻止列表，请点击位于该页顶部工具栏中的 *"导入"*。这会打开导入列表页。使用位于该页的 *"浏览"*按钮来寻找文本文件，该文件包含了您希望导入的地址，然后请点击 *"导入列表"*。

该文本文件每行必须只能有一条地址，您应该使用标准的文本编辑器 (比如 Notepad)来创建它，以防在不经意间插入了任何不常见的格式或者字符，从而防碍了导入过程。

使用 CSV 文件导入

如果您希望为每一条被导入的地址添加对应的注释，那么在您导入这些地址的时候，您将需要使用 CSV 文件，而不是一个简单的地址列表。您可以使用任何纯文本编辑器，比如 Notepad 来创建 CSV 文件。只需按以下格式创建文件并保存为*文件名.csv*。CSV 文件的第一行必须是映射行，以让 SecurityGateway 知道数据是按什么顺序出现的。文件中的每一项都必须包含在引号中，并以逗号分隔。

格式：

CSV 需要两列：*值*与*注释*。*"值"*列是用于您希望添加至阻止列表的邮件地址，而 *"注释"*列是用于关于每个条目您希望添加的任何批注。该列表中任何没有注释的条目，同样需要引号，引号中无内容，以表示该条目没有注释。

CSV 文件内容示例：

```
"Value","Comments"("值", "注释")
"myenemy@example.net","A comment about my enemy."("关于我敌人的注释")
"someone@example.org",""
"mister@domain.com","A comment about mister."("关于我先生的注释")
```

从阻止列表导出地址

要导出您的地址阻止列表：

1. 在页面顶部工具栏上点击 *"导出"*。这会打开文件下载对话框。
2. 点击 *"保存"*。
3. 选择文件名称和位置。
4. 点击 *"保存"*，然后是 *"关闭"*。

阻止列表条目

该页面用来向阻止列表添加新地址以及编辑现有的条目。只要您点击位于该列表顶部工具栏中的 *"新建"*或 *"编辑"*，就会打开这个页面。

列表项

电子邮件地址：

在第一个框中，输入您希望添加至阻止列表的邮件地址。您可以在地址的邮箱部分使用星号，以将该域的所有地址归入阻止列表。例如，"*@example.org"将把来自 example.org 任何发件人的所有邮件归入阻止列表。

注释：
在该区域可输入有关该条目的任意注释或说明，供自己参考。

保存与关闭
当您完成对条目的添加或编辑，请点击 *"保存并关闭"*以向阻止列表保存该条目。

关闭
如果您希望关闭阻止列表条目页面同时不作任何保存，请单击该按钮。

2.3 查看我的隔离区

隔离区是 SecurityGateway 认为太可疑而未投递的那些入站邮件的保留位置。它有助于防止接收大量垃圾邮件或其他可疑或不需要的邮件。被隔离的邮件保留在 SecurityGateway 服务器上，您可登录服务器并进行查看、删除邮件，或从隔离区释放邮件以将其按正常方式投递给自己。为帮助您管理隔离区，SecurityGateway 将定期向您发送邮件以便您了解隔离文件夹的内容。隔离区设置可在我的设置 31 页面上进行管理。

并非所有用户都可访问隔离区或修改隔离区设置。

隔离区的每一条目分成数列，分别列出了邮件被隔离的日期和时间、发件人、收件人以及主题等。此外还有几列描述了邮件被隔离的原因、邮件大小及邮件分数 (这是 SecurityGateway 用于识别垃圾邮件的内部分数)。

在隔离区页面顶部的工具栏上有数个按钮，可用于执行以下任务：

- **刷新**—点击该按钮刷新隔离区，以显示自您开始查看隔离区以来可能新增的邮件。
- **搜索**—使用丰富的搜索功能来过滤隔离区，以便只显示特定邮件。可基于邮件隔离原因进行搜索，搜索报头中的特定文本，搜索所有日期或日期起至范围等等。要搜索隔离区：点击工具栏上的 *"搜索"*按钮以打开搜索窗口，然后选择搜索条件，最后点击该窗口内的搜索按钮执行搜索。搜索结果会出现在搜索窗口下方—过滤隔离区以便只显示匹配搜索参数的邮件。要隐藏搜索窗口同时保留下方的过滤结果，可在工具栏上再次点击 *"搜索"*。搜索执行完毕，在搜索窗口内点击 *"取消"*使隔离区页面恢复常态。
- **查看**—选择一则邮件，然后点击该按钮可打开邮件信息屏幕。该屏幕有三个选项卡：记录、邮件和来源。记录选项卡包含投递过程的记录，它是描述 SecurityGateway 和发送该邮件的服务器或客户端之间通信详情的技术性日志。邮件选项卡包含邮件的实际内容，来源选项卡包含邮件的来源，其中包括邮件报头、html代码等。
- **释放**—选择一则邮件，然后点击该按钮从隔离区将其释放以进行投递。
- **允许列表**—选择一封邮件，并点击该按钮来将发件人或收件人添加到您的允许列表 33。
- **删除**—选择一则邮件并点击该按钮将其删除。
- **阻止列表**—选择一封邮件，并点击该按钮来将发件人添加到您的阻止列表 35。
- **全部删除**—点击该按钮删除全部隔离邮件。

.

2.4 查看我的邮件日志

邮件日志包含了所收发的每一邮件条目。它列出了邮件的处理日期和时间，发件人和收件人，以及邮件主题。此外，还列出了投递结果，如是否被投递、隔离或拒绝，若未投递还会提供原因，如发件人被列入阻止列表，邮件包含受限制的附件等等。最后，每一条目还列出了邮件大小及其分数。SecurityGateway 内部使用邮件分数来确定该邮件是否为垃圾邮件的可能性。

并非所有用户都可访问邮件日志。

在邮件日志页面顶部的工具栏上有数个按钮，可用于执行以下任务：

- **刷新**—点击该按钮刷新邮件日志，以显示自您开始查看日志以来可能新增的条目。
- **搜索**—使用丰富的搜索功能来过滤邮件日志，以便只显示特定邮件。可基于是入站邮件还是出站邮件来搜索日志，搜索报头中的特定文本，搜索所有日期或日期起至范围等等。要搜索邮件日志：点击工具栏上的 *"搜索"*按钮以打开搜索窗口，然后选择搜索条件，最后点击该窗口内的搜索按钮执行搜索。搜索结果出现在邮件日志页面中。要隐藏搜索窗口同时在日志页面上保留搜索结果，可在工具栏上再次点击 *"搜索"*。搜索执行完毕，在搜索窗口内点击 *"取消"*使邮件日志页面恢复常态。
- **详情**—选择一则邮件，然后单击该按钮可打开邮件信息屏幕。该屏幕有三个选项卡：记录、邮件和来源。记录选项卡包含投递过程的记录，它是描述 SecurityGateway 和发送该邮件的服务器或客户端之间通信详情的技术性日志。邮件选项卡包含邮件的实际内容。其可用性取决于邮件的保存时间，是否投递成功，以及是否将 SecurityGateway 设为保留该数据。来源选项卡包含邮件的来源，其中包括邮件的报头、html代码等。若邮件较老或 SecurityGateway 未设置为保存该信息，则来源可能不可用。
- **重新投递**—选择该列表中的一封或多封邮件，然后点击此按钮来进行重新投递。使用 Ctrl+Click 或 Shift+Click 以选择多封邮件。仅当邮件内容尚未从数据库中删除时，才能使用该选项。
- **垃圾邮件**—选择一则邮件并单击该按钮将邮件标记为垃圾邮件。这可帮助 SecurityGateway 以后更为精确地识别垃圾邮件。在某些情况下或当 SecurityGateway 未设置为支持该选项时，可能无法使用该按钮。
- **非垃圾邮件**—选择一则邮件并点击该按钮将邮件标记为非垃圾邮件。这有助于防止 SecurityGateway 以后错误地将合法邮件标识为垃圾邮件。在某些情况下或当 SecurityGateway 未设置为支持该选项时，可能无法使用该按钮。
- **允许列表**—选择一个条目，并点击该按钮来将发件人或收件人添加到您的允许列表 33。
- **阻止列表**—选择一个条目，并点击该按钮来将发件人或收件人添加到您的阻止列表 35。

章节

3

3 设置/用户

"*设置/用户*"菜单有九个部分，包含链接通往 SecurityGateway 的核心配置选项。您将使用这些部分中的选项以设置您的域与用户账户、邮件投递选项、隔离设置、备份与数据库首选项，以及其他一些配置选项。以下是对各个部分的简单概述。要了解更多详情，请参见这部分的概述或者每部分下的各个页面。

账户 41

账户部分位于 *"设置/用户"*菜单之下，包含了关于您的 SecurityGateway 用户账户与域的选项。该部分之下有五个与账户相关的链接，它们包括一些选项用于创建域与用户账户，指定用户验证来源，为一系列用户选项设置默认值等等。

邮件配置 65

"邮件配置"部分提供链接通往四个页面，用于管理各种与邮件相关的功能。例如，您将使用这部分的选项来指定您用户的邮件账户所位于的服务器，设置您的隔离区选项，配置各种邮件投递选项以及管理其他的技术性设置。

归档 78

归档部分提供了与存储和搜索通过 SecurityGateway 的邮件相关的选项。

安全通信 90

SecurityGateway 新的 "安全通信"功能为您的用户提供了一种向其域外的收件人发送安全邮件的方式，通过这种方式，邮件绝不会离开 SecurityGateway 服务器。它通过使用安全的通信网络门户来实现这一点。发送邮件后，收件人会收到一封电子邮件通知，告知他们有可用的安全邮件，其中包含用于创建安全邮件收件人 91 账户的链接，以便他们可以查看位于您 SecurityGateway 服务器上的邮件。通过收件人的浏览器访问安全邮件，并通过 HTTPS 加密在 SecurityGateway 服务器和收件人之间维护端到端的加密。

免责声明（报头/脚注） 95

邮件免责声明是服务器可以动态添加到入站、出站和本地邮件正文上方或下方的文本部分。使用该页面来创建和管理您的免责声明。

系统 100

系统部分位于 "设置/用户"菜单之下，包含链接通往各种系统功能页面，例如加密设置、HTTP 界面选项、目录位置、磁盘空间管理选项等等。

数据库 115

这部分的选项处理 SecurityGateway 保存的数据类型与数量，有自动备份选项，还有些选项用于自备份文件恢复服务器。

软件更新 120

使用此页面来检查是否存在可用的 SecurityGateway 更新版本。您可以手动地检查更新或使用一个选项，让 SecurityGateway 自动检查更新。在找到一个更新时，您可以通过网络界面下载并进行安装。

注册 121
注册页面列出了您的产品注册信息，包括注册该产品的人名或公司，注册码以及您注册的状态。

3.1 账户

账户部分位于设置/用户 40菜单之下，包含了关于您的 SecurityGateway 用户账户与域的选项。在该部分中有五个与账户相关的链接：

域 41 与 用户 46—使用域列表与用户列表来管理您的域和用户。要打开域列表，请点击*导航菜单左窗格上的*"设置/用户"，然后点击*该窗格中"账户"部分*下的"域和用户"。在选中一个域的情况下，通过点击域列表工具栏上的*"用户"*按钮可以显示用户列表。

管理员 50—使用管理员列表来管理在 SecurityGateway 中被指定的所有全局管理员及域管理员。全局管理员能够完全控制 SecurityGateway 中的所有设置及选项，甚至还能管理其他管理员账户及设置。域管理员能够访问他们有权限的域的所有设置与选项。他们不能编辑全局设置或者访问其他域所特有的设置。

用户验证源 52—该页面用来管理您所有的用户验证源，用户验证源是用来确认未知本地地址的有效性。每次有入站邮件的收件人是一个未知的本地用户，SecurityGateway 会查询用户验证源的用户域配置来验证该未知地址是否合法。如果地址有效，SecurityGateway 将为该地址创建用户账户，并试图将邮件投递到所在域的域邮件服务器 66。如果该地址无效，则将拒收邮件。

自动创建域 60—使用该页面来指定您是否想要自动创建一个 SecurityGateway 的新域，每当一封入站邮件的收件人是一个未知域的未知用户，您默认的用户验证源可对其进行验证。

用户选项 60—使用 该页面来指定通过登录用户的 SecurityGateway 账户，用户能够访问的选项有哪些。可在全局范围内或按域设置"用户选项"。

3.1.1 域和用户

3.1.1.1 域列表

域列表用来管理您的域和用户。欲打开列表，请点击导航菜单左窗格上的*"设置/用户"*，然后点击该窗格中"账户"部分下的*"域和用户"*。您也可通过 SecurityGateway 设置页面右边域字段下的*"查看域"*链接以获得域列表。

域列表有两栏：名称和用户。名称栏列出了您的所有域，用户栏列出了属于每个域的用户帐户数。欲查看或编辑一个域的属性 43，请双击列表中所要的域。欲查看一个域的用户列表 46，点击相应域的用户链接。

页面顶部的工具栏用来启动与域列表相关的各项任务。大部分工具栏按钮要求您在点击所要使用的按钮前，先从列表中选中域。只有以下按钮例外：新建，导入和导出。这些按钮在点击之前无需选中域。工具栏中包含下列十个选项：

新建
点击 *"新建"*来打开属性 43 对话框，用于创建一个 SecurityGateway 的新域。您可在 *"属性"*栏中为域指定名称，邮件服务器以及其他想要的设置。

编辑
使用工具栏上的编辑按钮，以打开目前域列表中所选中域的相应属性 43 对话框。或者，您也可以双击一个条目来打开 "属性"对话框。

删除
欲删除一个或多个域，从列表中选中域然后点击 *"删除"*。会跳出一个框，要求您确认是否决定删除该域。在点击每个域时，您可按住 Ctrl 键来选中多个域。

显示/隐藏搜索
点击 *"显示搜索"*来打开 "域列表"的搜索选项。在 *"域名"*框中输入一些文本并点击 *"搜索"*来过滤 "域列表"，由此来仅显示包含该文本的域。点击 *"取消搜索"*来取消搜索，并将 "域列表"返回到常规状态。

用户
从域列表中选中一个条目然后点击工具栏上的 *"用户"*来打开域的用户列表 46。与域列表相似，用户列表用来管理一个域的用户账户。

邮件
该按钮用来打开选中域的邮件日志 254。邮件日志包含了为每封发送至/来自域的邮件而准备的条目。从邮件日志可打开任意条目的邮件信息页，它显示了 SMTP 会话记录及邮件的内容和来源 (可用时)。

隔离
点击 *"隔离"*来查看选中域的 "隔离 255"页面。该域的所有已隔离邮件都已列出并且在此页面上查看。

允许列表
使用 "允许列表"按钮来查看选定域的地址允许列表 213。

阻止列表
使用 "阻止列表"按钮来查看选定域的地址阻止列表 205。

导入
您可以使用一个以逗号分隔值 (CSV)的文件来将一组域导入到域列表中。为此，可在页面顶部工具栏上点击 *"导入"*。将打开导入域的对话框。使用该对话框上的 *"浏览"*来导航包含您所要导入的域的 CSV 文件，然后点击 *"导入域"*。

CSV 文件格式
您可以使用任意文本编辑器，例如记事本，来创建用于添加域至域列表的 CSV 文件。只需按以下格式创建文件并保存为 *文件名.csv*。

CSV 文件的第一行必须是映射行，以使服务器了解数据的排列顺序。支持映像行中的两个字段：域和最大用户。两个字段都必须包含于引号内并以逗号隔开。*"域"*字段表示域的名称（例如：example.com），而 *"最大用户"*字段表示该域所允许的最大用户账户数。所有域的名称必须包含于引号内，而且若指定了最大用户数的值，必须以逗号将域名称隔开。

CSV 文件示例：

```
"域", "最大用户"
"domain.com", 50
"example.com"
"example.org", 10
```

导出
通过点击域列表工具栏上的导出，从而导出您的域列表。将以与先前所说的用于导入选项的相同格式在 CSV 文件中列出您的域。欲导出域列表：

1. 在页面顶部工具栏上点击 *"导出"*。这会打开文件下载对话框。
2. 点击 *"保存"*。
3. 选择文件名称和位置。
4. 点击 *"保存"*，然后是 *"关闭"*。

3.1.1.1.1 域属性

属性对话框用来创建一个 SecurityGateway 的新域，或者用来编辑一个现有域。通过点击域列表[41]上的 *"新建"*来显示 "属性"对话框，或者选中一个条目然后点击 *"编辑"*。*"属性"*有四个选项卡：属性，验证，邮件服务器，管理员。

域管理员[50]可以通过只读形式访问验证源与邮件服务器列表。

属性

属性标签用于指定域名称，域所允许的最大用户帐户数以及一个验证密码。用户限制和密码是可选的。

域名：
在文本框内输入域名称。例如："example.com"，"domain.com"，等等。这是将用于每个用户邮件地址的域。

限制用户数
若您希望限制属于该域的用户数，点击该选择框然后在下方输入所希望的数字。默认情况下，禁用该选项。

最大用户：
若您希望限制属于该域的用户账户数，请启用上方的 *"限制用户数"*选项，然后在此处输入用户数。

限制邮件大小最大值
如果您希望为此域的邮件设置最大可接受的 SMTP 邮件大小，请选中此框并指定大小。默认情况下禁用该选项，并应用全局的可接受的最大 SMTP 邮件大小 76 限制。

SMTP 验证密码
若您希望为该域指定一个 SMTP 验证密码，请使用此选项。那么当通过 SecurityGateway 发送邮件时，您的用户或者域邮件服务器 66 便可使用该密码来验证。欲使用该密码来验证，将域当作登录/用户名凭证来使用。例如，若域是 "example.com"并且您在此选项中指定了 "1234Password"，那么您将使用以下两个凭证来验证："example.com"和 "1234Password"。若您将密码选项设为空，那么任何一名发件人，若其仅使用域名称作为用户名来验证都将失败。

若管理员想要使用 CRAM-MD5 验证，SMTP 验证密码同样有用。此类型的验证要求 SecurityGateway 知道密码；且不能使用用户验证源。

在多数情况下，每个用户会仅仅使用他/她自己帐号的邮件地址和密码作为验证凭证，但是有一些邮件服务器的配置可能要求域邮件服务器有其自己的凭证，或者要求多名用户来分享一个验证凭证组。提供了此选项以兼容这种类型的需求。

绑定域到 IP 地址
如果您希望将域绑定到特定的 IP 地址，请选中此框并在提供的空格中输入 IP 地址和主机名。来自该域的邮件将从该 IP 地址发送。也可以为域指定 HELO 字符串或 SMTP 主机名。当向该域发送邮件时，该值是在 SMTP/HELO 指令中使用的全称域名 (FQDN)。对于入站连接，除非多个域绑定到相同的 IP 地址，否则将使用此值，在这种情况下，使用的 FQDN 将与按字母顺序排在第一位的域关联。

域别名
使用此选项为域指定任何别名。假定域的所有用户对每个域别名有效。如果某个域已注册了多个域名 (例如：altn.com、altn.us、altn.biz 等等)，这十分有用。

验证

验证标签用于分配将用于域的用户验证源 52 。若到达该域的邮件的地址指向一名未知用户，将查询这些源以确认该地址是否合法。若找到了该地址，那么将为此收件人创建一个 SecurityGateway 的账户。

不查询验证源，将手动管理用户
如果您不想为特定域查询任何验证源，请勾选此选框。在这种情况下，必须对该域手动管理所有用户。

可用源：
此框中列出了您先前创建的所有可用用户验证源。要为该域分配一个源，那么请从清单中选中源然后点击 "-->"箭头。

选中源：
此框中列出了您分配到此域的所有验证源。要从域中删除一个源，那么请从清单中选中源然后点击 "-->"箭头。

首选项：向上/向下
以验证源出现在选中源列表中的顺序对其进行查询。要将一个源移动到一个较高/较低未知，点击此源，然后使用向上向下箭头使其移动到想要的位置。

一旦出现了正面或负面的结果，SecurityGateway 将接受此结果并停止查询源。例如，如果列出了三个验证源且第一个验证源指出用户不存在，SecurityGateway 将会接受该结果并拒绝邮件，而不去查询另两个验证源。然而，若发生非致命错误，例如因验证源暂时出现故障，那么将以 *4xx* 错误代码拒绝邮件，以指示发件人稍后重试。

新建
如果您需要为该域创建一个新的用户验证源来使用，请点击 *"新建"*来打开新的用户验证源[55]屏幕。创建了新源后，它将出现在可用源列表中。

邮件服务器

邮件服务器标签用于分配将用于域的域邮件服务器[66]。当邮件到达此域中的一个已验证用户，SecurityGateway 将试图将邮件投递至此处所列出的选中服务器，以它们所列的顺序来放置。

可用域：
此框中列出了您先前创建的所有可用的域邮件服务器。要为该域分配一个服务器，那么请从清单中选中服务器然后点击 "-->"箭头。

选中的服务器：
此框中列出了您分配到此域的所有域邮件服务器。要从域中删除一个服务器，那么请从清单中选中服务器然后点击 "-->"箭头。

首选项：向上/向下
SecurityGateway 会试图将邮件以服务器出现在选中服务器列表的顺序投递至域邮件服务器。要将一个服务器移动到一个较高/较低位置，点击此服务器，然后使用向上向下箭头使其移动到想要的位置。

不使用此邮件服务器投递域邮件，仅可分配给特定的域用户
如果您选择一个服务器并点击此框，则该服务器将不会用于投递域的邮件——它将被指定为 "[USER ONLY]"。如果您希望使用该服务器为特定用户投递邮件，请使用 "用户编辑 » 属性[48]"页面上的 "邮件投递"选项来将服务器分配给用户。

新建
若您需要为该欲创建一个新的域邮件服务器来使用，请点击 *"新建"*来打开新的邮件服务器[66]屏幕。创建了新服务器后，它将出现在可用服务器列表中。

管理员

管理员标签用来分配有权管理此域的管理员[50]。由于全局管理员已有权管理所有域，因此在此处未将其列出。

可用管理员：
此框中列出了您之前指定的所有可用域管理员，不论其控制的是哪个域。要给予管理员权限来配置此域，那◆◆请从清单中选中管理员然后点击“-->”箭头。

选中的管理员：
此框中列出了有权限管理该域的所有域管理员。要删除某人访问此域的管理员级别，那么请从清单中选中管理员然后点击“-->”箭头。

新建
如果您需要为该域创建一个新的管理员，请点击*“新建”*来打开新建管理员[51]屏幕。创建了新管理员后，它将出现在已选管理员列表中。

3.1.1.2 用户列表

用户列表用于管理域用户账户。要打开该列表，请在左窗格中的导航菜单上点击*“设置/用户”*，然后在右窗格中用户和管理员栏目下，点击想查看的用户列表所在域。也可通过“域列表[41]”中的每个域条目转到用户列表。

用户列表有三栏：启用，姓名和邮箱。启用栏针对每个用户项包含一个复选框，可用于快速启用/禁用该用户的账户。姓名栏列出了用户的真实姓名（如 Frank Thomas），邮箱栏列出了用户邮件地址中的邮箱部分（如 "frank@example.com" 中的 "frank"）。要编辑用户，可双击列表中的所需用户或选择用户，然后单击页面顶部工具栏上的编辑按钮。这会打开用户编辑[48]屏幕。

页面顶部的工具栏用于启动与用户列表相关联的各项任务。大多数工具栏按钮要求首先从列表中选择用户，然后才能单击所需按钮。只有以下按钮例外：后退、新建、导入和导出。这些按钮无需选择用户即可单击。工具栏包含下列 11 个选项：

返回
当通过域列表[41]打开用户列表时，使用该按钮可轻松转回上一页。

新建
点击*“新建”*打开“新建用户[48]”对话框，用于在域下创建新用户账户。类似于“用户编辑[48]”对话框，在*“新建用户”*中可指定用户的邮箱名、真实姓名、密码和管理员权限。

编辑
使用工具栏上的编辑按钮可打开与用户列表中当前选定的用户对应的用户列表[48]。另外，还可通过双击用户项打开用户编辑对话框。

删除
要删除一个或多个用户，可从列表中选择用户，然后点击*“删除”*。接着会出现一个对话框，要求您确认删除用户的决定。使用 Ctrl 和 Shift 键可选择多个用户。

显示/隐藏搜索
点击*“显示搜索”*来打开“用户列表”的搜索选项。在*“用户名或邮箱”*字段中输入一些文本并点击*“搜索”*来过滤“用户列表”，由此来仅显条目中示包含该文本的用户。点击*“取消搜索”*来取消搜索，并将“用户列表”返回到常规状态。

设置
该按钮打开选定用户的我的设置[31]页面，用于更改用户密码，设置账户的隔离首选项，启动用户的自动允许列表，并指定用户登录 SecurityGateway 时每页显示的项目数。

邮件
该按钮用于打开选定用户的邮件日志[254]。邮件日志为该用户收发的每封邮件包含一个条目。从邮件日志可打开任意条目的邮件信息页，它显示了 SMTP 会话记录及邮件的内容和来源（可用时）。

隔离
点击 *"隔离"*可查看选定用户的"隔离[255]"页。该用户所有被隔离的邮件都罗列在该页上，可供审核。

允许列表
使用 "允许列表"按钮可查看选定用户的地址允许列表[213]。这是用户的个人允许列表，仅应用于他或她的账户。

阻止列表
使用 "阻止列表"按钮可查看选定用户的地址阻止列表[205]。这是用户的个人阻止列表，仅应用于他或她的账户。

导入
可使用逗号分隔值（CSV）文件将一列用户导入用户列表。为此，可在页面顶部工具栏上点击 *"导入"*。这会打开导入用户对话框。使用该对话框上的 *"浏览"*按钮找到包含要导入用户的 CSV 文件，然后点击 *"导入用户"*。

在导入用户对话框底部是选项：*"自动创建不存在的域。"*启用该选项时，若导入的用户列表中包含的电子邮件地址指向不存在的域，将自动创建新域。若禁用该选项，则指向 SecurityGateway 中不存在域的地址将被忽略，相应条目不会导入。

CSV 文件格式
可使用任意文本编辑器（如 Notepad）创建 CSV 文件以便将用户添加到用户列表。只需按以下格式创建文件并保存为*文件名.csv*。

CSV 文件的第一行必须是映射行，以使服务器了解数据的排列顺序。映射行中支持以下字段：

- **电子邮件**（Email）- 用户的电子邮件地址，例如 "frank@example.com"。
- **邮箱**（MailBox）- 电子邮件地址的邮箱部分（即 "frank@example.com" 中的 "frank"）。
- **域**（Domain）- 地址的域部分（即 "example.com"）。
- **全名**（FullName）- 用户的真实姓名，例如 "Frank Thomas"。
- **密码**（Password）- 用户的密码，用于登录账户或通过 SecurityGateway 发送邮件时进行身份验证。
- **启用**（Enabled）- 指定是否启用或禁用账户。可在该字段中使用 "1"、"yes" 或 "true" 来启用账户，或使用 "0"、"no" 或 "false" 来禁用账户。

电子邮件、邮箱和域字段按顺序处理，因此若其中任一字段值与前一字段冲突，则将使用后一字段值。例如，若在电子邮件字段中使用 "frank@example.com"，但随后在域字段中使用 "domain.com"，那么将使用 "frank@domain.com" 作为邮件地址。

各行中的所有字段都必须用引号括起来，并用逗号分隔。

CSV 文件示例：

```
"Email", "MailBox", "Domain", "FullName", "Password", "Enabled"
"frank@example.com", "frank", "example.com", "Frank Thomas",
"1234Password", "1"
"rip@example.com", "rip", "example.com", "Rip Collector",
"FoundAPenny", "yes"
"big@domain.com", "big", "domain.com", "Mister Big", "NumeroUno",
"1"
```

导出
单击工具栏上的导出按钮可导出域用户列表。它将使用与上述导入选项相同的格式把列表导出到 CSV 文件。要导出用户列表：

1. 在页面顶部工具栏上点击 *"导出"*。这会打开文件下载对话框。
2. 点击 *"保存"*。
3. 选择文件名称和位置。
4. 点击 *"保存"*，然后是 *"关闭"*。

3.1.1.2.1 用户编辑

用户编辑屏幕用于在 SecurityGateway 域下创建新的用户账户或编辑现有账户。通过在用户列表 46 页面上点击 *"新建"* 按钮或选择一个条目并点击 *"编辑"* 可打开该屏幕。在 *"用户编辑"* 页面上，可指定邮箱名、用户名、密码，以及该用户是否也是 "管理员 50"。您还能指定希望与用户关联的任何别名。

属性

该账户被禁用
如要禁用该账户，可点击该复选框。当账户被禁用时，SecurityGateway 不会接受该用户收发的任何邮件

邮箱名：
该选项用于指定用户的邮箱名和域（例如 frank@example.com）。这是用户的电子邮件地址，在登录其 SecurityGateway 账户时会用到。当配置用户的邮件客户端使用 SMTP 身份验证时，它亦用作该客户端的 *"用户名"* 或 *"登录"* 参数。

真实姓名：
该选项用于指定用户名（如 "Frank Thomas"）。

密码：
该密码用于登录用户账户及进行 SMTP 身份验证。

密码（确认）：
每当输入新密码时，必须使用该区域确认密码输入无误。

已为此用户设置本地密码——请点击此处来清除密码
当为用户设置了本地密码时，将显示此邮件。如果您希望删除该密码，请使用“**点击此处来清除密码**”链接。没有本地密码的用户只能使用支持其域验证的用户验证源[52]来进行验证。

此账户无需强密码
如果您希望为账户免除强密码[63]要求，请勾选此框。

管理员设置

账户是一名管理员
创建或编辑用户账户时，若希望用户是全局或域管理员[50]，可点击该复选框并选择以下选项之一。

全局管理员
“全局管理员[50]”可完全掌控 SecurityGateway 中的所有设置和选项，乃至其他管理员账户和设置。因此，指定账户为“全局管理员”时应慎重。

域管理人
“域管理员”可对拥有管理权限的域上所有相关设置和选项进行访问。他们无法编辑全局设置或访问其他域的特定设置。指定域管理员时，必须选择至少一个*“可用域”*供用户管理。

可用域：
该列表框列出了所有 SecurityGateway 域，其上可授予用户域管理员访问权限。要使用户控制其中的一个或多个域，可从列表中选择该域并点击“-->”箭头。

选定域：
该列表框列出了所有 SecurityGateway 域，其上已授予用户域管理员访问权限。要从列表中删除域，可将其选中，然后点击“<---”箭头。

可以创建域
如果您希望允许域管理员创建新域并将其添加为域管理员，请选中此框。

域创建限制：[xx]域
允许域管理员在创建新域时，使用此选项设置允许他或她创建的域的数量限制。

邮件投递

使用域邮件服务器
默认情况下，用户的邮件将由被分配至用户域[43]的域邮件服务器处理。如果您希望选择特定的邮件服务器来处理此用户的邮件，而不是使用域分配的服务器，请选择以下选项。

使用指定的邮件服务器投递邮件
如果您选择此项，会将该用户的邮件发送到指定的服务器，而不是发送到分配给用户域的任何域邮件服务器。

可用/选定服务器
如果您希望指定一个服务器来处理用户的邮件，请从列表中选择一个可用的服务器，并使用箭头将其移动到选定的服务器。

别名

点击"别名"选项卡来指定您希望与用户关联的任何别名。您还可以将您希望转换为别名的现有 SecurityGateway 用户合并，而不是单独的用户。

别名：
要为用户分配别名，请在提供的空白处输入电子邮件地址，然后点击"添加"。要从列表中删除别名，请选择所需条目然后点击"删除"。

合并用户：
当您希望将其他用户转换为与此用户关联的别名时，请使用"合并用户"选项。当用户验证源错误地导致单独的 SecurityGateway 用户被创建时，如果地址实际上是已经存在的用户的别名，则需要这样做。

通过在"合并用户"框中键入电子邮件地址，可以快速找到要合并的地址。用户列表将在您输入时被过滤，只显示与您输入内容相匹配的地址。

"合并用户"链接
在"合并用户"列表中，请点击与您希望转换为别名的地址相关联的合并用户链接。关联的地址将被移动到别名列表。

3.1.2 管理员

管理员列表用于管理在 SecurityGateway 中指定的全局管理员、域管理员和隔离区管理员。

全局管理员能够完全控制 SecurityGateway 中的所有设置及选项，甚至还能管理其他管理员账户及设置。因此，指定账户为"全局管理员"时应慎重。

"域管理员"可对拥有管理权限的域上所有相关设置和选项进行访问。他们无法编辑全局设置或访问其他域的特定设置。当指定一个域管理员时，您必须选中至少一个域让用户管理。

隔离区管理员可以查看和管理对域有访问权限的用户隔离队列。

管理员列表中有三栏：启用，电子邮件以及真实姓名。启用栏里包含了一个每个条目的选择框，可以用来快速地启用/禁用管理员账户。电子邮件栏列出了管理员的电子邮件地址，用其登录到 SecurityGateway—管理员账户并不一定要是 SecurityGateway 其中一个域里的本地账户。真实姓名栏列出了用户的真实姓名（例如：Frank Thomas）。要编辑一名管理员，双击列表中想要的条目或者选中它然后点击页面顶部工具栏上的"编辑"选项。将会打开编辑管理员 51 屏幕。

页面顶部的工具栏包含了下列四个选项：

新建
点击 *"新建"*打开新建管理员屏幕，它是用来创建一个新的管理员账户。该屏幕等同于 "编辑管理员[51]"屏幕。

编辑
使用工具栏上的 "编辑"按钮，以打开目前列表中选中条目的相应 "编辑管理员[51]"屏幕。此外，您还可通过双击一个条目来打开该屏幕。

删除
要删除一个或多个管理员，从列表中选中条目然后点击 *"删除"*。会跳出一个框，要求您确认是否决定删除管理员。您可以使用 "Ctrl 和 Shift"键来选择多个条目。

针对域：
使用 *"针对域："*通过下拉列表框来选择在列表中要显示哪位管理员。默认显示了所有管理员，不过您可以选择 "--全局--"，仅显示一名全局管理员；或者从列表中选择一个域，仅显示域管理员。

3.1.2.1 编辑管理员

"编辑管理员"屏幕用于编辑现有的全局管理员、域管理员或隔离区管理员，也可以新建一个。点击 *"管理员"*页面上的***[50] "新建"或者选中列表中的一个条目然后点击 *"编辑"*，便可显示此屏幕。在 *"编辑管理员"*选项中，您会指定该管理员是与本地账户相对应还是该管理员是一个外部用户，然后您便可提供管理员本地邮箱或者外部邮件地址，密码以及全称。您也可以指定该用户是否是全局管理员、域管理员或隔离区管理员。

属性

本地用户 — 本地域成员
如果管理员账户与您 SecurityGateway 其中一域的一个本地账户相对应，那么请选择该选项。

外部 -非本地域成员
管理员无需与一个本地用户账户相对应。她们可以是有外部邮件地址的外部用户。如果您想要指定该管理员为外部用户，那么请选择该选项。

邮箱或邮件地址
如果您选择了上方的 *"本地用户"*选项，你将为管理员输入一个邮箱，然后从下拉列表框中选中一个本地域。如果您选择了 *"外部"*选项，那么您只要输入管理员的外部邮箱地址。在上述两种情况下，管理员的邮件地址是用来登录到 SecurityGateway。

全名：
使用该空间来输入管理员姓名 (例如：Frank Thomas)。

密码：
这是管理员用来登录到 SecurityGateway 时所用的密码。

密码 (确认)：
每当输入一个新的密码，您必须在此框中重新输入新密码以确认是否输入正确。

该账户被禁用
若您想要禁用管理员账户，请点击此选择框。

类型

使用这些选项来指定管理员类型：全局管理员、域管理员或隔离区管理员。

全局管理员
"全局管理员[50]"可完全掌控 SecurityGateway 中的所有设置和选项，乃至其他管理员账户和设置。因此，指定账户为"全局管理员"时应慎重。

域管理人
"域管理员"可对拥有管理权限的域上所有相关设置和选项进行访问。他们无法编辑全局设置或访问其他域的特定设置。指定域管理员时，必须选择至少一个*"可用域"*供用户管理。

隔离区管理员
隔离区管理员可以查看和管理对域有访问权限的用户隔离队列。

可用域：
该框中列出了域或隔离区管理员能够访问的所有 SecurityGateway 的域。要让管理员能够控制这些域中的一个或多个，请从列表中选择域然后点击"-->"箭头。

选定域：
该框中列出了域或隔离区管理员能够控制的所有 SecurityGateway 的域。要从列表中删除域，可将其选中，然后点击"<---"箭头。

可以查看域用户邮件的内容/来源
该选项根据您在数据库 | 数据保留[116]中的设置，应用到 SecurityGateway 已保留的邮件。将始终保留排队等待投递到域邮件服务器的邮件和隔离的邮件。此项不应用于已归档的邮件。

可以创建域
如果您希望允许域管理员创建新域，请选中此框。管理员将被自动添加为他或她创建的任何域的域管理员。默认情况下，禁用该选项。

域创建限制：[xx]域
当允许域管理员创建域时，默认情况下最多可以创建五个域。您可以将此限制更改为希望允许的任何数字，如果您不想设置限制，则可禁用该选项。

3.1.3 用户验证源

该页用于管理所有用户验证源，它们可确认未知本地地址的有效性。要打开该页面，请在左窗格中的导航菜单上点击*"设置/用户"*，然后在该窗格的账户部分下点击*"用户验证源"*。

每当有入站邮件发往未知本地用户，SecurityGateway 都会查询为该用户所在域配置的用户验证源，以验证未知地址是否合法。如果地址有效，SecurityGateway 将为该地址创建用

户账户，并试图将邮件投递到所在域的域邮件服务器[66]。如果地址无效，邮件将被拒绝。每当以这种方式创建了新账户，可以向此用户发送欢迎邮件[60]，其中包含 SecurityGateway 的登录链接。

对于来自未知本地用户的出站邮件，SecurityGateway 将查询所在域的用户验证源，其处理方式与入站邮件完全一致。此外，当用户试图使用其邮件地址和密码验证连接时，SecurityGateway 将把这些验证凭据传递到用户验证源。若用户未通过身份验证，邮件将被拒绝。若身份验证成功，则将接受邮件用以投递，并为该用户创建 SecurityGateway 账户。对于已经存在的帐户，SecurityGateway 将首先在本地用户数据库中核对用户的登录凭证。若未发现匹配项，则再检查验证源。

用户验证源按其在域属性[43]屏幕验证选项卡上的罗列顺序进行查询。一旦得到正或负结果，SecurityGateway 将接受该结果并停止继续查询。例如，如果列出了三个验证源且第一个验证源指出用户不存在，SecurityGateway 将会接受该结果并拒绝邮件，而不去查询另两个验证源。然而，若发生非致命错误，例如因验证源暂时出现故障，那么将以 *4xx* 错误代码拒绝邮件，以指示发件人稍后重试。

正确配置验证源以便只确认有效用户，这一点至关重要。若验证源是开放式中继或在某个 SecurityGateway 域上又被称为 "垃圾箱"，它将确认每封发往未知用户的入站邮件。这可能会导致创建许多错误的用户，因为大多数入站垃圾邮件所发往的无效用户都错误地通过了该验证源的验证。因而注册密钥的用户限制可能很快就达到了饱和。

页面上用户验证源每行一条，分以下四列：说明、主机、端口和类型。说明列用于描述验证源（例如 *"example.com 上的服务器 X"*）。该主机列列出了验证源的主机名或 IP 地址，端口列是每个验证源使用的端口，类型列是验证源的类型：SMTP 验证（呼叫转移）[56]、活动目录/Exchange[56]、MDaemon (Minger)[57]、MDaemon (XML API)[57]、LDAP[57] 或 Microsoft 365[58]。要编辑验证源，可双击它或选中后在页面顶部工具栏上点击 "编辑"。这将打开编辑用户验证源[55]屏幕。

除 LDAP 之外的所有验证类型都支持动态身份验证。当用户试图进行身份验证或登录 SecurityGateway 时，将首先核对 SecurityGateway 本地登录凭证，但若本地项不存在，则再将其登录凭证传递到验证源以进行身份验证。这使得用户无需记住单独的一组 SecurityGateway 专用凭证，即可进行身份验证或登录其 SecurityGateway 账户。

当使用 CRAM-MD5[76] 方式进行身份验证时，无法动态验证 AUTH 密码。

页面顶部的工具栏包含以下五个选项：

新建
点击 *"新建"* 来打开 "新建用户验证源" 屏幕，用于创建新验证源。该屏幕类似于编辑用户验证源[55]屏幕。

编辑
使用工具栏上的编辑按钮打开与列表中当前选定项对应的编辑用户验证源[55]屏幕。此外，您还可通过双击一个条目来打开该屏幕。

删除
要删除一个或多个验证源，可从列表中将其选中，然后点击 *"删除"*。随后出现一个对话框，要求您确认删除验证源的决定。您可以使用 "Ctrl 和 Shift"键来选择多个条目。

验证用户
当在 *针对域：* 下拉列表框中选择 "- 全部 --"时，点击该按钮会使 SecurityGateway 立即尝试验证所有用户—甚至包括在过去某一时刻已验证过的用户。将删除用户验证源无法验证的任何用户（包括手动添加的用户）。当在 *针对域：* 列表框中选择了特定域，SecurityGateway 将只尝试验证该域的用户。

选项
打开用户验证源选项页面来激活响应缓存，并标记用户在指定时间后重新验证。

标记用户在 [xx] 小时后重新验证
如果用户仍然存在，此选项通过定期询问验证源来协助维护用户列表。在指定小时数后，验证过的用户在下次发送或接收电子邮件时被标记为重新验证。不删除被禁用的用户。

缓存消极响应长达 [xx] 分钟
当对验证源的查询显示账户不存在时，此选项会将结果缓存长达指定的分钟数。这有助于限制对验证源进行冗余查询的次数。

始终查询外部别名的默认用户验证源
启用此项时，将通过查询默认用户验证源来验证所有未知地址。如果用户验证源返回的地址是本地域用户的外部别名，则将在必要时创建本地用户，并将别名与该用户关联。使用该功能需要定义至少一个默认用户验证源。

> 由于所有未知地址都需查询，因此可能会执行大量查询操作。

针对域：
使用 *"针对域："* 下拉列表框选择在列表中显示哪些用户验证源。默认显示所有验证源，但可选择 "-- 默认 --"以只显示（在 编辑用户验证源[55] 对话框中）指定的默认验证源，或从列表中选择一个域以只显示该域的验证源。

3.1.3.1 用户验证源选项

标记用户在 [xx] 小时后重新验证
如果用户仍然存在，此选项通过定期询问验证源来协助维护用户列表。在指定小时数后，验证过的用户在下次发送或接收电子邮件时被标记为重新验证。不删除被禁用的用户。

缓存消极响应长达 [xx] 分钟
当对验证源的查询显示账户不存在时，此选项会将结果缓存长达指定的分钟数。这有助

于限制对验证源进行冗余查询的次数。

始终查询外部别名的默认用户验证源
启用此项时，将通过查询默认用户验证源来验证所有未知地址。如果用户验证源返回的地址是本地域用户的外部别名，则将在必要时创建本地用户，并将别名与该用户关联。使用该功能需要定义至少一个默认用户验证源。

由于所有未知地址都需查询，因此可能会执行大量查询操作。

还请参阅：

用户验证源 52

3.1.3.2 编辑验证源

使用编辑用户验证源屏幕可编辑现有用户验证源 52 或创建新验证源。通过在用户验证源页面上点击 *"新建"* 或从列表中选择一项并点击 *"编辑"* 可打开该屏幕。在该屏幕上可指定验证源的类型、位置、连接端口、所需身份验证凭证以及使用该验证源验证用户的 SecurityGateway 域。

属性

类型：
使用该下拉列表框指定该项验证源所用的用户验证方式：SMTP 验证（呼叫转移）56、活动目录/Exchange 56、MDaemon (Minger) 57、MDaemon (XML API) 57、LDAP 57 或 Microsoft 365 58。下方的 *说明*、*主机或 IP* 以及 *端口* 选项应用于全部四类验证源。其余选项根据所选择的类型而各不相同。对于所有验证类型，当未知本地用户通过验证时，将为其创建 SecurityGateway 账户，并可以向该新账户发送欢迎邮件 60，其中包含 SecurityGateway 的登录链接。然后可使用该用户的邮件地址和密码登录其 SecurityGateway 账户以查看邮件日志、邮件隔离区等等。因为 LDAP 不支持动态身份验证，因此若选择该验证类型，则必须为用户提供 SecurityGateway 密码，以便他们能登录 SecurityGateway。

除 LDAP 之外的所有验证类型都支持动态身份验证。当用户试图进行身份验证或登录 SecurityGateway 时，将首先核对 SecurityGateway 本地登录凭证，但若本地项不存在，则再将其登录凭证传递到验证源以进行身份验证。这使得用户无需记住单独的一组 SecurityGateway 专用凭证，即可进行身份验证或登录其 SecurityGateway 账户。

当用户的域被配置为使用 Microsoft 365 用户验证源，并且用户正在登录到 SecurityGateway 界面时，用户将被重定向到 Microsoft 365 授权 URL 以完成登录过程。一旦成功登录 Microsoft 365，会将该用户的浏览器重定向回 SecurityGateway。

> 当使用 CRAM-MD5 [76] 方式进行身份验证时，无法动态验证 AUTH 密码。

描述：
该文本框用于描述验证源（例如 *"example.com 上的服务器 X"*）。它对应于用户验证源 [52] 页面上的 *"描述"*列。

主机或 IP：
这是验证源的主机名或 IP 地址。当查询该验证源时，SecurityGateway 会连接到此位置。该选项对应于用户验证源页面上的 *"主机"*列。

端口：
这是 SecurityGateway 连接验证源时使用的端口，它对应于用户验证源页面上的 *端口*列。

SMTP 验证（呼叫转移）

若希望使用 SMTP 验证入站邮件的未知本地收件人和出站邮件的未知本地发件人，请选择该类型。类似于回叫验证 [169]，SecurityGateway 将试图通过 SMTP 协议验证用户。对试图进行身份验证的未知本地发件人，SecurityGateway 将把该用户的凭证传递给 SMTP 验证源用以身份验证。若身份验证成功，SecurityGateway 将接受邮件用以投递，并为该用户创建账户。对于已经存在的帐户，SecurityGateway 将首先在本地用户数据库中核对用户的登录凭证。若未发现匹配项，则再检查 SMTP 验证源。

要求身份验证
若 SMTP 验证源要求进行身份验证，请点击该复选框。然后填写下面的用户名和密码。

用户名：
若 SMTP 验证源要求进行身份验证，请在此指定用户名。

密码：
在此输入 SMTP 验证源密码。

活动目录/ Exchange

若希望使用活动目录或 Exchange 服务器验证未知本地用户，请选择该类型。如同上述的 SMTP 验证，该验证类型也支持动态身份验证。对试图进行身份验证的未知本地发件人，SecurityGateway 将把该用户的凭证传递给活动目录/ Exchange 服务器用以身份验证。若身份验证成功，SecurityGateway 将接受邮件用以投递，并为该用户创建账户。对于已经存在的帐户，SecurityGateway 将首先在本地用户数据库中核对用户的登录凭证。若未发现匹配项，则再检查 SMTP 验证源。

用户名：
该区域是登录验证源所需的活动目录/Exchange/Windows 用户名。

密码：
在该区域输入与上面指定的活动目录/Exchange 用户名对应的密码。

搜索过滤器：
这是在活动目录/Exchange 服务器上查询用户时所用的搜索过滤器。大多数情况下默认搜索过滤器应已够用。

MDaemon (Minger)

若希望使用以 Minger 为用户验证源的 MDaemon 服务器，请选择该验证类型。这是扩充后 MDaemon 服务器专用的 Minger 协议，因此该选项不能用于其他类型的服务器。与以上两种验证类型一样，它也支持动态身份验证。这意味着用户可使用其邮件服务器登录凭证进行身份验证或登录 SecurityGateway 账户。

要求身份验证
若 MDaemon 服务器要求进行身份验证以使用 Minger，请点击该复选框。

密码：
在此输入 MDaemon 服务器的 Minger 密码。

MDaemon (XML API)

选择此选项可将 MDaemon XML-API 用作用户验证源类型。MDaemon 的 XML API 为 Minger 提供了更好的替代方案，因为它可以使用可逆加密对 MDaemon 未存储密码副本的账户进行身份验证。它还能在一次调用中返回账户的所有别名。**注意：**该选项需要 MDaemon 23.0.2 或更高版本。

MDaemon XML API URL:
MDaemon 的安装默认 XML-API URL 是：
"http://servername:RemoteAdminPort/MdMgmtWS/"不过，强烈建议在 MDaemon 中配置 HTTPS 选项来使用安全的 HTTP (例如 https://servername:RemoteAdminPort/MdMgmtWS/)。

创建 MDaemon XML API服务账户
在 SecurityGateway 内配置此“用户验证源”时，该进程将创建“MDaemon XML API服务账户”。MDaemon XML API 支持权限受限的服务账户。当配置“用户验证源”来使用 MDaemon XML API 时，SecurityGateway 将调用 MDaemon XML API 来创建一个服务账户，该服务账户仅被授予执行用于验证用户账户的“XMINGER”操作的权限。创建该服务账户需要 MDaemon 全局管理员的凭证。SecurityGateway 在创建服务账户后，不会保留 MDaemon 全局管理员的凭证。返回的服务账户凭证用于这个“用户验证源”。

LDAP

若希望使用 LDAP 服务器来验证用户，请选择该验证类型。然而，不同于其他验证类型，无法使用 LDAP 验证用户的登录凭证。因此不支持动态身份验证或“即时”身份验证。结果，若要求用户进行身份验证，则由 LDAP 验证源验证的用户在不使用 SecurityGateway 账户密码的情况下无法登录 SecurityGateway 或通过它发送邮件。

绑定 DN：
输入可访问 LDAP 服务器的识别名 (DN)，以便 SecurityGateway 能利用它来查询用户名。这是绑定操作中用于身份验证的识别名。

密码：
该密码连同*“绑定识别名”*值将被传递到 LDAP 服务器用于身份验证。

基底项 DN：
这是目录信息树 (DIT)中的根 DN 或起点，SecurityGateway 将在此搜索活动目录以查找用户。

搜索过滤器：
这是在 LDAP 服务器上查询用户时所用的 LDAP 搜索过滤器。大多数情况下默认搜索过滤器应已够用。

搜索范围：
这是 LDAP 搜索范围或区域。

仅基底识别名
若希望搜索范围仅限于上面提供的*基底项 DN*，请选择该选项。搜索不会深入到目录信息树 (DIT)中该点的以下部分。

基底识别名的下一级
若希望将搜索扩展到 DIT 中 *"基底项 DN"*的下一级，请使用该选项。

基底识别名及其所有子识别名
该选项把搜索范围从 *"基底项 DN"*扩展到其所有子项，直至 DIT 中的最低子条目。默认选择该选项。

Microsoft 365

如果您希望将 Microsoft 365 用作用户验证源，请选择此验证类型，然后按照以下步骤进行设置。

若要允许 SecurityGateway 访问 Microsoft 365 租户，Microsoft 365 计划需要 Exchange Online。请确保 Microsoft 365 计划包括此功能。

要将 Microsoft 365 用作用户验证源，SecurityGateway 要求服务主体已被授予访问 Microsoft 365 租户的权限。此外，Microsoft 365 使用 "Azure 活动目录"作为其目录服务。以下步骤详细介绍了如何在 SecurityGateway 中将 Microsoft 365 配置为用户验证源。

使用 Microsoft Identity 平台来注册应用程序：

1. 登录到 Microsoft Entra 管理中心。

   对于具有多个租户的账户，请点击 "设置"图标并选择所需的租户。
2. 在 "管理中心"菜单，请选择 "身份 > 应用程序 > 应用程序注册"。
3. 选择 "新建注册"
4. 在名称字段中输入应用程序名称。
5. 选择 "注册"
6. 记下应用程序 ID
7. 选择 "API 权限"

8. 选择 "添加权限"
9. 选择 Microsoft Graph
10. 选择 "应用程序权限"
11. 选择 "**Group.Read.All**"和 "**User.Read.All**"
12. 选择 "添加权限"
13. 点击 "授予管理员同意..."按钮
14. 点击 "是"
15. 选择 "证书 & 密钥"
16. 点击 "新建客户端密钥"
17. 在描述字段中输入描述
18. 选择单选按钮来确定密码的有效期。
19. 请记下在 "值"字段中生成的密码，因为该密码无法再次查看。

在 SecurityGateway 中：

1. 使用全局管理员登录 SecurityGateway
2. 选择 "设置/用户"
3. 选择 "账户"
4. 选择 "用户验证源"
5. 点击 "新建"
6. 选择 **Microsoft 365**
7. 输入描述
8. 在 "域名"字段中输入 Microsoft 365 域名。
9. 选择 "类型"

   对于大多数配置，该选项将是 "全局"。
10. 输入 Azure AD 的 "**Service Principle**"字段中的 "应用程序 ID"。

    这可以在 Azure AD 中 "应用程序注册"的 "概述"页面上找到
11. 输入上述 Azure AD 的 "密码"字段中生成的密码。
12. 点击 "保存并关闭"。

类型

该服务器为默认用户验证源
若希望将该验证源指定为默认用户验证源，请点击该复选框。未专门指定验证源的所有 SecurityGateway 域使用默认用户验证源。自动域创建 60功能也使用这些默认用户验证源。

在下面指定使用此用户验证源的域...
使用以下选项将该验证源分配给一个或多个 SecurityGateway 域。若域上分配了多个验证源，则可在域属性屏幕的验证[43]选项卡上指定它们的查询顺序。

可用域：
该框列出了所有可用的 SecurityGateway 域。要指定利用该验证源的域，请从列表中将其选中并单击 "--->" 箭头。

选定域：
该框列出了所有 SecurityGateway 域，它们被配置为利用该验证源验证用户。要从列表中删除域，请将其选中并单击 "<---" 箭头。

3.1.4 自动创建域

使用该页面来指定您是否想要自动创建一个 SecurityGateway 的新域，每当一封入站邮件的收件人是一个未知域的未知用户，您默认的用户验证源[52]将对其进行验证。要打开此页面，请点击导航菜单左窗格上的 *"设置/用户"*，然后点击该窗格中 "账户"部分下的 *"自动域创建"*。

配置

启用自动创建域
启用后，每当一封入站邮件指向的是一个未知域的未知地址，那么 SecurityGateway 将查询您的默认用户验证源。如果该地址为有效地址，SecurityGateway 将会同时创建域和用户。自动创建域需要定义至少一个默认用户验证源[55]，由于要对所有未知地址进行查询，则会进行大量的查询。默认情况下禁用此功能。

在使用此项功能时，很重要的一点是，您的验证源配置正确，能够验证唯一的有效用户。举例来说，如果验证源是一个开放中继，那么每一封发送至一个未知域或用户的入站邮件都将通过此验证源来验证。这可能导致创建了多个错误的域和用户，而这些都是由发送至无效地址的入站垃圾邮件所引起的。

3.1.5 用户选项

在该页面上指定用户登录 SecurityGateway 账户后能访问哪些选项。可在全局范围内或按域设置 "用户选项"。

访问控制

允许用户修改密码
该选项允许用户通过我的设置[31]页修改其 SecurityGateway 账户密码。

显示密码字段的“显示密码”图标
每个密码字段均包含一个眼睛图标，用户可以点击该图标来查看他刚在该字段中键入的密码。如果您不想让用户看到他们的密码，请禁用此选项。

允许用户查看和管理自己的隔离文件夹
启用该选项时，用户可查看并管理隔离区中自己的入站邮件。这使他们可访问查看我的隔离区[37]页面以释放邮件、删除邮件或进行其他操作。

允许用户修改自己的隔离设置
点击该选项使每个用户可在我的设置[31]页面上编辑隔离设置。

允许用户查看其账户收发邮件的日志
这使每个用户可通过 SecurityGateway 中的查看我的邮件日志[38]链接查看其账户的邮件日志。日志中列出了该用户的邮件地址收发的所有邮件。

允许用户查看邮件记录
在启用此项时，用户可以在其邮件日志[38]或隔离区[37]中查看邮件的记录详情。禁用此项时，只有管理员可以查看该记录。默认情况下，禁用该选项。

允许用户搜索和查看发送至或来自其账户的归档邮件
默认情况下，用户可以搜索和查看发往其账户或来自其账户的已归档邮件。如果您不这样做，请清除此复选框，以允许他们执行此操作。

> **允许用户删除发送至或来自其账户的归档邮件**
> 如果您允许用户删除来往其账户的已归档邮件，请勾选此框。默认情况下，禁用该选项。

允许用户对发往其账户的邮件禁用反垃圾邮件测试
若希望允许用户在发往其账户的邮件上禁用反垃圾邮件测试，请点击该选项。当用户在“我的设置[31]”页上禁用其账户的反垃圾邮件测试时，DNSBL[134]、URIBL[137]、启发式和贝叶斯[129]以及爆发保护[126]垃圾邮件测试都不会执行。

允许用户为其账户禁用“账户劫持检测”
默认情况下，用户无法控制他们的账户是否免于账户劫持检测[181]。如果您希望允许用户控制该选项，请启用此选项。

允许用户启用“双重验证”
如果您希望允许用户配置其账户，以便在登录 SecurityGateway 账户时要求“双重验证”，请选中此框。启用后，用户使用安全的 HTTPS 连接从浏览器登录，双重验证[29]页面将出现在“我的账户”选项的下方。“双重验证”是一个额外的安全层，要求您在登录时使用不同的身份验证方法进行第二次身份验证。例如，您可以使用密码登录，然后使用设备的指纹识别器，或输入由手机上的验证器应用程序生成的特殊安全代码进行第二次身份验证。

> **允许 WebAuthn 用于双重验证**
> 如果您希望允许用户使用 Web Authentication API（也称为 WebAuthn）来进行双重验证，请选中此框。WebAuthn 允许用户使用生物识别技术、USB 安全密钥和蓝牙等进行身份验证。这将使用其双重验证[29]页面上的选项来设置他们首选的验证方式（该页面仅在用户通过 HTTPS 访问 SecurityGateway 时对他们可用）。

为了安全起见，您不能对 "无密码登录"和 "双重验证"同时使用相同的验证方法。因此，如果您希望同时使用这两种方法，请为每种方法选择不同的身份验证方法。

请访问：**webauthn.guide** 来获取有关 WebAuthn 如何运作的更多详细信息。

允许用户启用 "双重验证"电子邮件验证
如果您希望允许用户在设置 "双重验证"时，在 SecurityGateway 中输入备选的电子邮件地址，这样他们就能通过电子邮件接收验证码，而不必使用 Google 身份验证器应用程序，那么请勾选此框。如果您不希望通过电子邮件允许验证代码，请禁用此选项。

通过邮件发送的双重验证码在：[xx]分钟
当通过电子邮件接收双重验证的代码时，这是用户在代码到期之前必须输入代码的时间。默认情况下将此项设置成 **10** 分钟。

要求用户启用 "双重验证"
如果您希望要求所有用户在登录时使用 "双重验证"，请选中此框。启用此选项后，用户首次签名时，将显示 "设置双重验证"页面。

允许每台设备记住用户 (需要 HTTPS)
启用此项时，每当用户通过安全的 HTTPS 连接进行连接时，将在登录页面上显示 *"在此设备上记住我"*这个选项。如果用户选中了该框，则从那时起，只要在完成操作后仅关闭浏览器而不使用 "退出"选项，并且在同一设备上打开 SecurityGateway，他就会自动登录。如果他退出，那么下次连接时他将必须再次登录。用户被记住的天数将在下方的 *"天数..."*选项中指定。之后将要求他再次登录。默认情况下禁用此项。**注意：**只要 "记住我"选项在当前设备或浏览器上处于活动状态，在用户的我的账户 » 设置 31 页面上就提供 *"在该设备/浏览器上不记住我"*这个选项。他们可以点击该链接取消在设备上 "记住我"。

将记住用户的天数 (从 1 到 365)
在使用 *"允许按设备记住用户"*这个选项时，这是在需要再次登录之前将记住用户的天数。默认情况下将此值设置成 30。

登录选项

在登录屏幕上显示 "忘记密码"链接
默认情况下，"忘记密码"链接出现在登录页面上，可用于通过电子邮件将链接发送给用户来更改他或她的密码。该链接将通过电子邮件发送到与 SecurityGateway 用户账户关联的地址。如果您不希望在登录页面上显示 "忘记密码"链接，请清除此复选框。

允许 WebAuthn 用于登录
如果您希望允许用户使用 Web Authentication API (也称为 WebAuthn)进行登录，该 API 允许用户使用生物识别技术、USB 安全密钥、蓝牙等进行身份验证，从而为用户提供安全、无密码的登录体验，那么请选中此框。用户可以在其我的账户 » 设置 33 页面上注册其无密码登录凭证。

请访问：**webauthn.guide** 来获取有关 WebAuthn 如何运作的更多详细信息。

在登录屏幕上显示以下管理员联系信息
如果您希望在登录页面上包含一些管理员的联系信息或链接，请激活此项并在框中输入一些文本。您在框中输入的文本可以包含一些 HTML，如锚点和图像。

默认值

对发往该账户的邮件不执行反垃圾邮件测试
如果您希望该选项管理我的设置[31]页面上相同名称用户选项的默认设置，请勾选此框。启用时，服务器默认对发往该账户的邮件不执行 DNSBL[134]、URIBL[137]、启发式和贝叶斯[129]以及爆发保护[126]垃圾邮件测试。

禁用此账户的"账户劫持检测"
如果默认情况下希望账户免于账户劫持检测[181]功能，启用此选项。在短时间内合法发送大量邮件的账户可能需要豁免。您可以在账户设置[31]页面上为个别账户设置此选项。

将接收我所发邮件的地址用户自动列入允许列表
该选项管理每个用户的我的设置[31]页面上*自动将我发送邮件的目的地址列入允许列表*这一选项的默认设置。当启用用户的这一选项时，该用户所发邮件的每一目的地址都将添加到其地址允许列表中，可通过 允许列表[33]这个链接进行访问。这有助于确保以后从这些地址发往用户的入站邮件不会被错误地标记为垃圾邮件。

要求强密码
默认情况下，所有新密码都必须包含至少八个字符，并且至少包含以下各项之一：

- 大写字符
- 小写字符
- 数字
- 特殊字符（例如．;,_.?/-=）

提供一个*"不为此账户要求强密码"*选项，位于"用户编辑[48]"页面上，您可以使用此项来为用户免除这个要求。

何时显示统计图表
使用此选项可以选择何时将统计图显示在仪表盘[9]和登录页面[28]上。您可以选择自动、始终、手动或从不。

语言
使用此下拉式列表来设置服务器发送系统生成的邮件时使用的默认语言。个人可以使用相应的用户选项来替代自己的设置。

对照来自第三方服务的已泄露密码列表检查密码
SecurityGateway 可以对照来自第三方服务的已泄露密码列表来检查用户的密码，并且无需将密码传输到该服务即可执行此操作。如果用户的密码出现在列表中，并不表示该账户已被黑客入侵。而是意味着某人在某处使用了与他们的密码相同的字符，并且发生

了数据泄露事件。从未在其他任何位置使用过的唯一密码更加安全，因为黑客在字典攻击中可能会使用已公开的密码。请参阅Pwned Passwords (已泄露密码)获取更多信息。

使用下拉菜单来选择自上次检查密码以来，您希望多久对列表进行一次密码检查。您可以选择：

- 从不 (不对照该列表检查密码。这是默认设置。)
- 自上次检查以来的一天
- 自上次检查以来的一周
- 自上次检查以来的一月

每页显示的项目数
该选项决定了在用户登录 SecurityGateway 时，每页将显示的条目数量，例如允许列表中的地址，邮件日志中的条目等等。每页底部的控件用于当项目太多而无法显示在一个页面上时转到其他页面。该选项默认值为 50。

使用条款

要求用户在登录之前接受以下使用条款
如果您希望每次登录 SecurityGateway 时都要求用户接受文本，例如使用条款声明，请启用此选项并在框中输入文本。用户可以通过勾选一个框来接受该声明。

新用户

向新用户发送欢迎邮件
若希望每当创建新用户时都发送 "欢迎"邮件，请启用该选项。该邮件提供了到 SecurityGateway 的链接，以便用户登录并管理账户首选项和隔离文件夹。默认情况下，禁用该选项。

创建新用户时向全局管理员发送警报
每当创建新的用户账户时，如果您希望向全局管理员[50]发送邮件，请勾选此框。

对照第 3 方已泄露密码列表检查新用户的密码
选中此框后，将使用上方的 "对照已泄露密码列表检查密码..."这个选项来检查新用户的密码。

允许用户邮箱名称包含加号 (+)字符
如果需要创建邮箱名称包含加号(+)字符的用户，请启用此选项。如果启用，这些邮箱将不会被视为子地址别名。例如，frank.thomas+billing@example.com 将被视为其自己的用户，而不是 frank.thomas@example.com 的别名 (请参阅下方的子寻址[64])。

子寻址

子寻址 (也被叫做 *plus addressing*)，是一种常用于将标签或文件夹名称附加到电子邮件地址的方法。使用此系统，被指向 *user+tag@domain* (例如 *frank.thomas+billing@example.com*)的邮件可以被自动路由到该地址中包含的账户的文件夹中。有些电子邮件服务器会自动执行此操作，有些会简单地将地址视为别名，还有一些可能根本不支持子寻址，将该地址视为常规的电子邮件地址，而不是地址加上一个标签。

例如在一个支持子寻址的服务器上，如果 frank.thomas@example.com 有一个 IMAP 邮件文件夹名为 "billing"，那么指向 "frank.thomas+billing@example.com"的到达邮件将被自动路由到该特定的文件夹中。如果服务器将子寻址视为别名，则邮件将被投递到 Frank 的收件箱（但是 Frank 可以创建一个电子邮件过滤器，以自动将该邮件放入他的 "billing"文件夹中）。如果服务器不支持子寻址，则该邮件将被拒收，将其视为被指向未知用户 "frank.thomas+billing"。

在 SecurityGateway 中，当入站邮件指向该类型的地址时，SecurityGateway 会检查是否存在邮箱名中包含 "+"字符的用户，或者它是否是用户的子寻址别名。如果未找到用户或别名，或者找到了用户但到了重新验证他们[54]的时间，那么将查询合适的用户验证源[52]。用户验证源查询将使用 SecurityGateway 收到的完整地址。这样做是为了确保邮件服务器将接受该地址。如果验证了该地址，则 SecurityGateway 将按需创建新用户或用户的别名。

最后，在将邮件投递到域邮件服务器[66]时，SecurityGateway 将始终使用原始邮件中所包含的完整邮件地址，例如 "frank.thomas+billing@example.com"。

例外 - 域

当配置这些设置时，如果您在页面顶部的 *"针对域："* 下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。请点击相应域的 *"查看/编辑"* 链接以查看或编辑其用户选项设置，或点击 *"重置"* 将域设置重置为默认全局值。

3.2 邮件配置

"设置/用户" 菜单下的 "邮件配置"部分提供转至以下5个页面的链接，其中提供各种相关邮件的功能：

域邮件服务器[66]——该页面是用来管理您所有的域邮件服务器的，SecurityGateway 将作为这些邮件服务器的网关而运作。通常您用户的邮件账户和他们的邮件都保存在这些服务器上。当 SecurityGateway 收到一封邮件，是发送至您某一域中经验证的用户的，它将尝试将邮件投递给与该域相关联的邮件服务器。

远程 POP 账户[68]—使用 "远程 POP 账户"选项可将 SecurityGateway 配置为使用 POP3 协议从远程 POP 邮箱下载邮件，以便重新分发给指定域的用户。收集完毕后，将根据 "编辑 POP 账户[68]"屏幕上提供的设置解析邮件，并投递给任何有效的用户，就像邮件使用传统的 SMTP 处理到达服务器一样。

隔离配置[71]——该页帮助您实现覆盖 *"……隔离邮件"* 选项，这些选项位于许多 "安全[124]"功能之下。此外，您可以选择您的用户是否可以在他们的域中各自覆盖默认的隔离选项，他们是否可以查看与管理他们隔离文件夹中的内容。最后，您还可以选择每隔多久之后您的用户将收到一封邮件，详述他们隔离文件夹中的内容。从不、每日或每周。

邮件投递[74]——位于邮件投递页面的选项，是用来指定是否让 SecurityGateway 自身来处理外发邮件的投递，或是交由另外的服务器来处理。该页还包括一些选项，控制 SecurityGateway 尝试投递那些发生非致命错误的接收与外发邮件时，在放弃投递并将邮件因其不可投递而返还给发件人前所花费的时间长短。这些选项是全局选项，适用于所有的 SecurityGateway 域。

邮件协议[76]——邮件协议页面包含了各种选项，用来管理 SecurityGateway 对邮件的技术性处理。例如，你将使用该页来指定将用作接收邮件的端口，所允许的最大并发 SMTP 会话的数量，SecurityGateway 是否会获准 VRFY 请求，您是否允许纯文本密码与其他一些类似的高级选项。

3.2.1 域邮件服务器

该页面是用来管理您所有的域邮件服务器的，SecurityGateway 将作为这些邮件服务器的网关而运作。通常您用户的邮件账户和他们的邮件都保存在这些服务器上。当 SecurityGateway 收到一封邮件，是发送至您某一域中经验证的用户的，它将尝试将邮件投递给与该域相关联的邮件服务器。每个SecurityGateway 域[41]将会有一个或多个与其有特定关联的邮件服务器，或使用您指定为默认服务器[66]的域邮件服务器。要打开 "域邮件服务器"列表，请点击导航栏上的 *设置／用户*，再点击 *邮件配置* 和 *域邮件服务器*。

域邮件服务器页面具有三列，每行列有一个条目。描述，服务器与端口。描述列用于对邮件服务器进行描述 (比如，*"Server X at example.com"*)。服务器列列出了主机名，IP 地址或邮件服务器。端口列列出了发送邮件时应该用到的端口。要编辑域邮件服务器，请双击条目或者选中它并点击页面顶部工具栏上的 "编辑"。这将打开编辑邮件服务器[66]屏幕。

页面顶部的工具栏包含了以下四个选项：

新建
点击 *"新建"*来打开新建邮件服务器屏幕，用于创建新的域邮件服务器。该屏幕与"编辑邮件服务器[66]"屏幕相同。

编辑
使用工具栏的 "编辑"按钮以打开"编辑邮件服务器[66]"屏幕，它对应列表内当前选择的条目。此外，您还可通过双击一个条目来打开该屏幕。

删除
要删除一个或多个域邮件服务器，请从列表中选择条目并点击 *"删除"*。会打开一个对话框询问您是否确定要删除这些服务器。您可以使用 "Ctrl 和 Shift"键来选择多个条目。

针对域：
使用 *"针对域："* 下拉列表框来选择列表中将显示的域邮件服务器。默认情况下会显示所有的服务器，但是您可以选择 "--默认--"来仅显示那些您已经指定为默认服务器的服务器 (位于 编辑邮件服务器[66]屏幕)或者从列表中选择一个域可以仅显示该域的邮件服务器。

3.2.1.1 编辑邮件服务器

编辑邮件服务器屏幕是用来编辑一个现有的域邮件服务器[66]或是创建一个新服务器。点击域邮件服务器页面上的 *"新建"*或是选中该页面上的一个条目然后点击 *"编辑"*，您便可得到

该屏幕。您将在该屏幕上提供此服务器的描述、位置、连接端口、任何所需的验证凭证以及 SecurityGateway 里使用该服务器的域。您也可以指定该服务器是否是默认的邮件服务器。

属性

描述：
使用此文本框来添加该服务器的描述（例如，*"Server X at example.com"*）。它与域邮件服务器 66 页面上的*"描述"*列相对应。

主机或 IP：
此选项针对于邮件服务器的主机名或者 IP 地址。当服务器试图将您的用户邮件投递至该位置时，SecurityGateway 将连接到该位置。该选项与"域邮件服务器"页面上的*"服务器"*列相对应。

端口：
这是 SecurityGateway 连接到服务器时所要使用的端口，它与"域邮件服务器"页面上的*"端口"*列相对应。

要求身份验证
若域邮件服务器要求您在发送邮件之前先验证，那么请点击此选择框。然后填写下面的用户名和密码。

用户名：
若服务器要求验证，在此指定您的用户名。

密码：
在此输入您的域邮件服务器密码。

类型

该服务器是一个默认的邮件服务器
若您希望该服务器成为您的默认域邮件服务器之一，请点击此选择框。默认服务器用于所有未与域邮件服务器有特别关联的 SecurityGateway 的域。

在下方指定应该使用此邮件服务器的域...
使用下方选项将该服务器分配至一个或多个 SecurityGateway 的域。若将多个域邮件服务器分配到一个域，那么随后您可以在域属性屏幕上的邮件服务器选项卡 43 指定尝试投递至这些域的顺序。

可用域：
该框列出了所有可用的 SecurityGateway 域。要指定使用该域邮件服务器的域，那么请从清单中选中域然后点击 "-->"箭头。

选定域：
此框中列出了您已配置的使用此邮件服务器的 SecurityGateway 所有域。要从列表中删除域，请将其选中并单击 "<---" 箭头。

3.2.2 远程 POP 账户

使用远程 POP 账户选项，将 SecurityGateway 配置为使用 POP3 协议——从远程 POP 邮箱下载邮件，并将邮件重新投递到指定域用户。收集完毕后，将根据编辑 POP 账户 68 屏幕上提供的设置解析邮件，并投递给任何有效的用户，就像邮件使用传统的 SMTP 处理到达服务器一样。

值得注意的是，存储在邮件箱中并且使用 POP3 协议检索邮件将缺少重要的路由信息（有时被称为邮件“信封”）如果这些邮件是使用了更加强大的 SMTP 协议来投递，那么将正常地提供这些信息。这是因为 POP 邮箱传统上意味着与个人而不是整个域或多个用户相关联——邮箱中的所有内容都假定针对同一收件人，因此不再需要初始路由信息。没有这个路由信息，SecurityGateway 会强制使用解析 70 选项来检查每封邮件的报头，试图确定预期的收件人。包含有关联的 SecurityGateway 域中的有效收件人的报头邮件将被发送。没有任何有效收件人的邮件将从 POP 邮箱中删除并从 SecurityGateway 中删除。

“远程 POP 账户”页面具有五列，每行列有一个条目。已启用、描述、主机、端口和域。要了解这些项目的详细信息以及如何创建和编辑 POP 账户条目，请参阅编辑 POP 账户 68 屏幕。

页面顶部的工具栏包含以下五个选项：

新建
点击 *“新建”*打开“新建 POP 账户”屏幕，它是用来创建一个新的 POP 账户条目。该屏幕等同于“编辑 POP 账户”屏幕。

编辑
使用工具栏的编辑按钮以打开“编辑 POP 账户 68 ”屏幕，它对应列表内当前选择的条目。此外，您还可通过双击一个条目来打开该屏幕。

删除
要删除一条或多个 POP 账户，从列表中选中条目然后点击 *“删除”*。会打开一个对话框询问您是否确定要删除这些条目。您可以使用 Ctrl 和 Shift 键来选择多个条目。

立即检查
点击此按钮立即检查选择的 POP 账户是否有新邮件。

针对域：
使用 *“针对域：”*通过下拉列表框来选择在列表中要显示哪些 POP 账户。默认情况下会显示所有账户，但您可以从列表中选择特定域以仅显示该域的 POP 账户条目。

3.2.2.1 编辑 POP 账户

使用 *“新建”*或 *“编辑”*选项（位于远程 POP 账户 68 页面）来打开“编辑 POP 账户”屏幕，用于创建或编辑您的 POP 账户条目。“编辑 POP 账户”屏幕包含两个选项卡：*“主机和选项”*以及 *“解析”*。“主机和选项”选项卡用于指定与 POP 账户关联的主机和登录信息，用于

连接 POP 主机的安全协议，以及指定 SecurityGateway 从 POP 账户收集邮件的频率。"解析"选项卡用于指定 SecurityGateway 将搜索收件人地址和发件人 IP 地址的报头。

主机和选项

该账户被禁用
如果您希望禁用 POP 账户，请勾选此框。该账户仍将在远程 POP 账户 68 列表上显示，不过 SecurityGateway 不再尝试从中收集邮件。清除复选框以再次从其中收集邮件。

为此域收集邮件
使用下拉列表指定与此 POP 账户关联的域。解析收件人地址的邮件报头时，SecurityGateway 将在这些报头中查找该域的用户。

邮箱

描述
使用该区域为 POP 账户提供姓名或说明。这仅供您参考，并出现在 POP 账户列表中。

主机名称或 IP
在此输入 POP 账户的域名或 IP 地址（例如：pop.example.com）。

端口
这是 SecurityGateway 从账户收集邮件时将使用的端口。默认的 POP 端口是 110。

用户名
在此输入 POP 账户的登录名或用户名。

密码
POP 账户的密码。

安全

使用安全连接
SecurityGateway for Email Servers 支持最新的加密技术来保护您的数据并保护连接。选择收集此 POP 账户邮件时希望使用的选项。

从不—如果 POP 主机不支持，或者您不想使用加密会话，请选择此选项。

TLS，若可用—如果您希望在从 POP 账户收集邮件时尽可能使用传输层安全（TLS）加密，请选择此选项。如果 POP 主机不支持 TLS，则 SecurityGateway 将正常收集邮件，而不使用加密。这是默认选项。

TLS—如果您希望在收集来自此 POP 账户的邮件时需要 TLS 加密，请选择此选项。

SSL—如果您希望在收集来自此 POP 账户的邮件时需要 SSL 加密，请使用此选项。

需要安全验证（APOP）
如果您希望在从此账户收集您的邮件时，使用 APOP 命令和 CRAM-MD5 验证，点击此框。这将使你不必再发送明文密码来认证。

邮件收集

将邮件留在服务器上
如果选择此项，SecurityGateway 将下载但不从 POP 账户的主机服务器中删除邮件。

...除非邮件存放日期超过以下天数
这是邮件在删除以前可以保留在 POP 主机上的天数。

有些主机可以限制在您的邮箱中存储邮件所允许的时间。

轮询间隔：[xx]分钟
此选项管理 SecurityGateway 将多久检查一次 POP 主机以查找新邮件。建议每五分钟检查一次。

超时：[xx]秒
这是 SecurityGateway 在放弃之前等待来自 POP 主机响应的秒数。建议设置成 60 秒。

解析

收件人 (RCPT)

为收件人解析这些报头 (RCPT)
使用此选项指定您希望 SecurityGateway 解析收件人电子邮件地址的标题。会检查此处列出的每个报头来获取地址。

为收件人解析这些“已接收”报头 (RCPT)
因为在邮件的 SMTP 信封中找到的收件人信息有时也可以在“已收到”邮件报头中找到，所以这可以使您可以分析这些邮件报头并可能收集实际的收件人地址。如果您希望解析来自于在邮件中所找到的所有“received”报头的有效地址，请点击此选框。

跳过最初的 [xx]“received”报头中隐藏软件版本标识
在一些服务器配置中，您可能希望解析 Received 报头不过需要跳过最初的几项。此设置允许你输入 SecurityGateway 将会在开始解析前跳过“received”报头的数量。

IP 地址

为发件人 IP 地址解析已接收报头
如果您希望解析来自于在邮件中所找到的所有“received”报头的发件人 IP 地址，请点击此选框。获取发件人的 IP 地址可用于各种安全性查找和垃圾邮件阻止选项。

跳过最初的 [xx]“received”报头中隐藏软件版本标识
在一些服务器配置中，您可能希望解析 Received 报头不过需要跳过最初的几项。此设置允许你输入 SecurityGateway 将会在开始解析前跳过“received”报头的数量。

为发件人 IP 地址解析此报头：
使用此选项列出您希望解析发件人 IP 地址的特定报头。默认值是 X-ORIGINATING-IP。

3.2.3 隔离区配置

隔离选项页面有助于您实现覆盖*"...隔离邮件"*选项，这些选项位于许多安全 124 功能之下；隔离区可以进行全局配置，也可以为特定的域配置。此外，您可以选择您的用户是否可以在他们的域中各自覆盖默认的隔离选项，他们是否可以查看与管理他们隔离文件夹中的内容。最后，您还可以选择每隔多久之后您的用户将收到一封邮件，详述他们隔离文件夹中的内容。从不、每日或每周。

邮件

在 SecurityGateway 服务器上保留被隔离的邮件
当选中该选项，任何邮件，只要匹配任一*"...隔离邮件"*的条件，这些条件会在安全 124 功能下指定，那么 SecurityGateway 服务器就会保留这些邮件。这是默认选项。

向用户发送列出他们隔离文件夹内容的邮件：
当邮件被保留在 SecurityGateway 服务器上的隔离区内，该选项决定了在每隔多久之后向您的用户发送一封邮件，该邮件列有他们隔离区中的内容。

从不
如果您不希望向每位用户发送这封列有他或她隔离文件夹内容的邮件，请选中该选项。

每 XX 小时
如果您希望在该时间间隔向用户发送隔离内容邮件，选择此选项并指定小时数。

每天
当选中该选项，每个帐户每天都将收到一封邮件，该邮件概述了此用户隔离文件夹的内容。这是默认选项。

每周
如果您希望每周发送此邮件一次，请选中该选项。

在下方指定的调度上：
点击 **"添加"**来打开 *"隔离报告调度程序"*，为何时发送隔离文件夹报告创建自定义调度。

调度

天
为调度创建新条目时，先选择您希望发送电子邮件的日期。您可以选择：每天、工作日（星期一到星期五）、周末（星期六和星期天）、或一周中的特定日子。如果您希望包含多个特定的日期，请为一周中的每一天创建一个单独的调度程序条目。

开始于...
输入您希望发送隔离报告的时间。时间值必须采用 24 小时格式，从 00:00 到 23:59。如果您希望全天定期发送报告，那么您还必须使用下方的 *"结束于..."*和 *"每隔 [xx] 分钟循环"*这两个选项。如果您希望此条目每天只发送一份报告，请留空 *"结束于..."*和 *"每隔...循环"*这两个选项。

结束于...
输入您希望定期报告电子邮件每天结束的时间。时间值必须采用 24 小时的格式，从 00:01 直到 23:59，且必须大于 *"开始于..."*值。例如，如果 *开始于...*时间值为 "10:00"，那么该时间值可以是 "10:01"到 "23:59"。如果您希望条目每天发送一份报告而不是重复报告，请留空此选项。

每隔 [xx]分钟循环
这是在指定的 *"开始于..."*和 *"结束于..."*时间之间发送隔离报告邮件的时间间隔。如果您希望条目每天发送一份报告而不是重复报告，请留空此选项。

仅包含自上次发送电子邮件以来被隔离的新邮件
默认情况下，每个隔离报告都包含隔离文件夹中包含的所有邮件的列表。如果您希望电子邮件仅包含自上次发送隔离报告以来已添加到隔离文件夹的邮件，请选中此框。如果报告中没有要包含的邮件，则不会生成隔离报告。

完成选择后，点击 "保存并关闭"来创建该条目并将其添加到 "隔离配置"页面。

按以下值排序隔离邮件：[已接收 | 发件人 | 主题 | 分值]
使用此选项可选择您希望如何对隔离电子邮件中包含的隔离邮件列表进行排序。默认情况下，列表按收到邮件的日期排序，但您也可以选择按发件人、主题或垃圾邮件分值排序。

在隔离邮件中包含 "查看邮件"选项
如果您希望在隔离报告电子邮件中包含 "查看邮件"这个选项，请选中此框，以允许用户查看其隔离邮件。该选项还位于：主页 » 我的账户 » 设置。

在隔离列表和邮件中包含 "始终允许"选项
默认情况下，隔离列表和隔离报告电子邮件中都有一个 "始终允许"选项。如果您不希望包含 "始终允许"这个选项，请取消勾选此框。

在隔离列表和邮件中包含 "列入阻止列表"选项
选中此项后，用户的隔离邮件列表和隔离报告电子邮件中将提供一个链接，该链接可用于将邮件发件人的地址添加到阻止列表中。

在隔离列表和邮件中包含"将域列入阻止列表"选项
选中此项后，用户的隔离邮件列表和隔离报告电子邮件中将提供一个链接，该链接可用于将邮件发件人的域添加到阻止列表中。

允许邮件服务器或者客户端过滤被隔离的邮件
选中该选项时，它将覆盖每个*"..隔离邮件"*选项，这些选项位于各种安全[124]功能之下。将要被隔离的邮件会再次发送给收件人，允许收件人的客户端或服务器隔离或过滤它们。通过使用位于该页顶部的*"域："*下拉列表框，您可以对该选项进行全局设置或为特定的域设置。

...用 [文本]标记主题
如果您希望向将要被隔离的邮件主题添加标签，请启用该选项。收件人的客户端或服务器可以使用该标签来过滤邮件。

...添加报头 [文本]
如果您希望向将要被隔离的邮件添加邮件报头，请启用该选项。收件人的客户端或服务器可以使用该报头来过滤邮件。默认报头是："X-Spam-Flag: (X-垃圾邮件-标记：)是"。

用户

以下两个选项与位于用户选项[60]页面的两个具有同一名称的选项相同。你在某一页上对设置作的任何更改都会复制到另一页上。在两个位置上都提供了这些选项仅为方便管理员进行设置。

允许用户查看和管理自己的隔离文件夹
启用该选项时，用户可查看并管理隔离区中自己的入站邮件。这使他们可访问查看我的隔离区[37]页面以释放邮件、删除邮件或进行其他操作。

允许用户修改自己的隔离设置
点击该选项使每个用户可在我的设置[31]页面上编辑隔离设置。

管理隔离（所有域）

使用这些选项，指定何时或是否向管理员发送列出管理隔离区内容的电子邮件。这些选项与上述用户的隔离报告选项相同。

例外 - 域

当配置这些设置时，如果您在页面顶部的*"针对域："*下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。在相应的域中点击*"查看/编辑"*链接来查看或者编辑其隔离选项设置，或点击*"重置"*来将域的设置重置回默认的全局值。

3.2.3.1 隔离报告调度程序

在隔离配置[71]页面上，位于*"在下方指定的调度上："*这个选项下方，请点击"添加"来打开"隔离报告调度程序"，为何时发送隔离文件夹报告电子邮件创建自定义调度。

调度

天
为调度创建新条目时，先选择您希望发送电子邮件的日期。您可以选择：每天、工作日（星期一到星期五）、周末（星期六和星期天）、或一周中的特定日子。如果您希望包含多个特定的日期，请为一周中的每一天创建一个单独的调度程序条目。

开始于...
输入您希望发送隔离报告的时间。时间值必须采用 24 小时格式，从 00:00 到 23:59。如果您希望全天定期发送报告，那么您还必须使用下方的 *"结束于..."*和 *"每隔 [xx] 分钟循环"*这两个选项。如果您希望此条目每天只发送一份报告，请留空 *"结束于..."*和 *"每隔...循环"*这两个选项。

结束于...
输入您希望定期报告电子邮件每天结束的时间。时间值必须采用 24 小时的格式，从 00:01 直到 23:59，且必须大于 *"开始于..."*值。例如，如果*开始于...*时间值为 "10:00"，那么该时间值可以是 "10:01"到 "23:59"。如果您希望条目每天发送一份报告而不是重复报告，请留空此选项。

每隔 [xx] 分钟循环
这是在指定的 *"开始于..."*和 *"结束于..."*时间之间发送隔离报告邮件的时间间隔。如果您希望条目每天发送一份报告而不是重复报告，请留空此选项。

仅包含自上次发送电子邮件以来被隔离的新邮件
默认情况下，每个隔离报告都包含隔离文件夹中包含的所有邮件的列表。如果您希望电子邮件仅包含自上次发送隔离报告以来已添加到隔离文件夹的邮件，请选中此框。如果报告中没有要包含的邮件，则不会生成隔离报告。

完成选择后，点击 **"保存并关闭"**来创建该条目并将其添加到 "隔离配置"页面。

3.2.4 邮件投递

"邮件投递"页面上的选项用于指定 Security Gateway 是自己处理出站邮件的投递，还是将该责任交给另一台服务器。该页面还包括一些选项，控制 SecurityGateway 重试[75]投递那些发生非致命错误的入站或出站邮件时，在放弃投递并将邮件作为不可投递邮件[76]，返还给发件人前所花费的时间频率。这些选项是全局选项，适用于所有的 SecurityGateway 域。

远程邮件投递

总是将所有外发邮件直接发送到收件人的邮件服务器
当选中该选项，SecurityGateway 将使用标准的 SMTP 投递过程以尝试将每封外发邮件直接投递到收件人的邮件服务器——将执行标准的 DNS 查询，检查 MX 记录等等。默认情况下，选中该选项。

总是将所有外发邮件发送到下列指定服务器
如果您希望将所有的外发邮件发送至另外的服务器，请选中这个选项以便使该服务器可以投递那些邮件。

邮件服务器：
使用该选项来指定 SecurityGateway 将所有的外发邮件发送到的邮件服务器，以让该服务器来处理邮件的投递。您可以输入一个主机或者 IP 地址，比如 "mail.example.com"或者 "192.168.0.1"。

端口
这是 SecurityGateway 将邮件发送至指定的服务器时，它将使用的端口。

访问以上邮件服务器需要验证
如果指定的邮件服务器需要验证，单击该选择框并输入以下的登陆信息。

用户名：
如果需要验证，在此处输入用户名登陆信息。

密码：
输入与以上输入的用户名对应的密码。

缓存 SMTP 连接故障：[xx]分钟发送摘要
默认情况下，将缓存 SMTP 连接故障长达 5 分钟。使用此选项可以调整它们将被缓存的时间，或者如果您不希望缓存它们，则禁用该选项。

重试队列

"重试队列"选项确定 Security Gateway 将如何处理由于某些非致命错误而无法投递的邮件，例如当收件服务器暂时不可用时。

第一个小时内，重试投递频率：每 [xx]分钟 (推荐：5)
在邮件无法投递之后的第一个小时内，这是 SecurityGateway 在进行进一步投递尝试前所等待的时间间隔。默认设置是 5 分钟。

如果邮件在此期间未投递，请通知发件人
默认情况下，如果 SecurityGateway 在一个小时内无法投递邮件，它将向发件人发送一封邮件，说明它未能投递邮件，但它将继续尝试。如果您不希望发送该邮件，请清除该复选框。

...在通知发件人时包含原始邮件
默认情况下，当 SecurityGateway 在第一个小时后向发件人发送 "无法投递"邮件时，它将包含原始邮件的副本。如果您不希望包含原始邮件，请清除该复选框。

...包含用于通知发件人的完整邮件记录
如果您希望在发送暂时或永久投递失败的未投递报告 (NDR) 时，包含完整的邮件记录，则启用此选项。默认情况下禁用此选项；仅会包含来自远程 SMTP 服务器的最终错误消息。

之后，重试投递频率：每 [xx]分钟 (推荐：240)
邮件在一小时内仍无法投递之后，SecurityGateway 将切换到此进一步投递尝试的时间间隔。默认设置是 240 分钟。SecurityGateway 将在以下 "无法投递邮件"选项中指定的天数内，按此间隔继续投递尝试。

缓存 SMTP 连接失败
默认情况下，当指向给定主机的 SMTP 连接失败时，SecurityGateway 将停止尝试连接到该主机，持续时间为比在上方 *"第一个小时内，重试投递频率：每 [xx] 分钟"* 这个选项中所指定的分钟数少一分钟。这样做可以防止 SecurityGateway 一再连接到一个离线主机，例如，有多个指定到该主机的邮件但是在进行首次投递尝试时，就发现该主机已关闭。如果您不希望缓存 SMTP 失败，请清除该复选框。

无法投递的邮件

不管是接收还是外发邮件，当这些邮件因为非致命错误，比如收件人的邮件服务器暂时不可用，而无法进行投递时，这些选项控制了 SecurityGateway 在放弃投递并将邮件返还给发件人前，将继续尝试投递邮件的时间长短。

如果邮件在 [xx] 天后仍无法投递，则暂停所有投递尝试 (建议：5)
这是 SecurityGateway 在放弃前将继续尝试投递邮件的天数。在此之后，它将停止投递尝试。

如果邮件无法传递，请通知发件人
默认情况下，在 SecurityGateway 停止投递尝试后，它会向发件人发送一封邮件，指出该邮件无法投递。如果您不希望发送该邮件，请清除该复选框。

...在通知发件人时包含原始邮件
默认情况下，当 SecurityGateway 向发件人发送 "无法投递" 邮件时，它将包含原始邮件的副本。如果您不希望包含原始邮件，请清除该复选框。

...包含用于通知发件人的完整邮件记录
如果您希望在发送暂时或永久投递失败的未投递报告 (NDR) 时，包含完整的邮件记录，则启用此选项。默认情况下禁用此选项；仅会包含来自远程 SMTP 服务器的最终错误消息。

3.2.5 邮件协议

邮件协议页面中包含了多个管理 SecurityGateway 邮件的技术处理选项。例如，你将使用该页来指定将用作接收邮件的端口，所允许的最大并发 SMTP 会话的数量，SecurityGateway 是否会获准 VRFY 请求，您是否允许纯文本密码与其他一些类似的高级选项。

服务器

HELO 域名：
这是在 SMTP 过程中 SecurityGateway 将用来识别其自身的域名 (例如：mail.example.com，smtp.domain.com，等等)。也将用于已接收报头，验证结果报头，以及其他需要准确识别哪个服务器正在处理邮件的地方。**请注意：** 如果您正在集群 111 环境中使用 SecurityGateway，您可以将此选项设置为集群中每台服务器上的唯一值。

SMTP 端口 (以逗号分隔)：
这是 SecurityGateway 将要接收 SMTP 邮件的端口。您可以列出多个端口，中间以逗号隔开。默认的 SMTP 端口是 25。

专用的 SSL 端口 (以逗号隔开)：
在此列出您接收邮件的专用 SSL 端口。您可以列出多个端口，中间以逗号隔开。默认的 SSL 端口是 465。

MSA 端口 (以逗号分隔)：
此项用于列出您的 MSA 端口。以逗号将多个端口隔开。默认的 MSA 端口是 465。

绑定套接字到这些 IPs (逗号分隔)：
若您希望将 SecurityGateway 绑定至特定的 IP 地址，在此列出这些 IP 地址并以逗号隔开。

最大并发 SMTP 入站会话数：
该值控制的是并发入站 SMTP 会话数，该会话数指的是在 SecurityGateway 开始以"服务器太忙"邮件来回应之前，它所接受的会话数。默认值为 100。

最大并发 SMTP 出站会话数：
在此输入的值是在发送邮件时，将会创建的并发出站 SMTP 会话的最大数。每个会话都会发送出站邮件，直至所有正在等候的邮件发送完毕。例如，若此选项设置的默认值为 30，那么可同时创建 30 个会话，允许 SecurityGateway 立刻试图投递 30 封不同邮件。

最大并发 POP 集合会话数
该值控制在服务器回应"服务器太忙"邮件前，可接收的最大并发 POP 集合会话的数量。

默认域：
从下拉列表框中选择域。当某人在没有包含域名的情况下试图登录，SecurityGateway 会假定使用的是该域。在没有指定域的情况下，执行 MAIL、RCPT 以及 VRFY 命令时也将使用该域。此外，当发送警告和邮件至外部管理员[50]时，SecurityGateway 将使用此域。

SMTP 协议设置

准许 VRFY 命令
如果您希望准许 VRFY[169] 命令，请使用此选项。默认情况下，禁用该选项。

允许纯文本密码 (不要求 SSL 或者 CRAM-MD5)
根据默认，SecurityGateway 将接受在 SMTP 验证过程中所发送的纯文本密码。若您禁用了此选项，那么就需要 SSL 或者 CRAM-MD5 的验证方式。

准许 CRAM-MD5 身份验证方式
启用了此选项后，SecurityGateway 将准许 CRAM-MD5 的验证方式。默认情况下，禁用该选项。

在答复和"Received:"报头中隐藏软件版本标识
如果您希望在服务器响应和"已接收："报头中隐藏 SecurityGateway 的软件版本信息，请勾选此框。默认情况下，禁用该选项。

为 RFC 符合性检查命令和报头
如果您希望拒收不符合 RFC 因特网标准的邮件，请启用此选项。启用后，SecurityGateway 将会以下邮件：包含控件参数或包含八位字符串参数的邮件，或者丢失日期，发件人或者发件人报头的邮件。此外，所要求的报头必须有一个相应的值—它们不能以空报头形式存在。如果您不希望拒收不符合标准的邮件，请清除此选择框。

允许一封邮件中有很多 RCPT 命令：[xx] (RFC says 100)
这是每封邮件所允许的 RCPT 命令数 (例如：收件人数量)。默认值为 100。

可接受的 SMTP 邮件的最大尺寸：[xx]KB (0 = 不限)
在此设置一个值将防止 SecurityGateway 接受超出某一固定大小的邮件。激活了此项功能后，SecurityGateway 将试图使用 RFC-1870 中所指定的 ESMTP SIZE 命令。若发送方支持 SMTP 扩闸名，那么 SecurityGateway 将决定邮件的大小优先于真实投递，并将立即拒收邮件。若发送方不支持此 SMTP 扩展名，那么 SecurityGateway 将允许发件服务器开始传输邮件，不过若稍后到达邮件的最大尺寸时会拒收该邮件。默认值"0"表示没有在邮件上放置尺寸限制。

断开连接如果数据传输超过：[xx]KB (0 = 不限)
若在 SMTP 连接过程中传输的数据超过该阈值，SecurityGateway 将关闭此连接。该选项的默认值为"0"表示没有大小限制。

链接超时：[xx]秒 (建议值：30)
这就是 SecurityGateway 在超时前等待 SMTP 连接的时间。

协议超时：[xx]秒 (建议值：300)
建立连接后，这是 SecurityGateway 等待主机开始 SMTP 协议会话的秒数。

循环检测和控制

最大邮件跳跃计数 (1—100)：
RFC 标准规定邮件服务器在处理邮件时，每次都必须盖印每封邮件。这些盖印可以累计，并作为一种权宜之计，来应对有时因错误配置而引起的循环邮件。若没有检测到，这些循环投递周期将耗费您的资源。通过计算邮件已处理的次数，能够检测到此类邮件并将其置于坏邮件 258 队列中。该选项的默认值是 20。

3.3 归档

3.3.1 配置

"电子邮件归档"捕获并保留通过 SecurityGateway 的所有邮件。管理员和最终用户都可以轻松地搜索 88 已归档邮件。

配置

启用邮件归档
如果您希望保存域的每封入站和出站邮件的副本，请选中此框。这些邮件被保存在归档存储中。每个归档存储 85 都是可搜索的 88，而且与一个域相关联。您可以使用右上角中的"针对域："下拉列表来覆盖个别域的这个设置。

接受"日记报告"并将转发邮件发送到此邮箱：
如果您希望指定一个或多个邮箱来接受 Microsoft 365 日记报告"或用于归档的其他转发邮件，请使用此选项执行此操作。SecurityGateway 将接受启用了归档的任何域的邮件，并通过解析报头来确定实际的收件人。此时，它将验证发件人或收件人是否为有效的本地用户（必要时查询相应的用户验证源），并验证域是否已启用归档，并将邮件添加到域的活动归档存储中。**请注意：**必须从域邮件服务器[66]来接收入站邮件。

启用电子邮件日志
启用此项可创建电子邮件日志报告。将为在下方的"**记录这些邮件**"选项中指定的邮件创建日志报告，并将这些报告发送至"**日志邮件地址**"。原始邮件将作为日志报告的附件原封不动地包括在内，而且日记报告的正文包含原始邮件中的信息，例如发件人电子邮件地址、邮件主题、邮件 ID 和收件人电子邮件地址。您可以选择记录*"仅内部邮件"*（默认设置）"、*"仅外部邮件"*或*"所有邮件"*。

归档存储

归档存储是包含已归档电子邮件的容器。每个归档存储都与一个域相关联。

自动创建归档存储
使用此选项来让 SecurityGateway 控制您归档存储的创建。这是建议的设置。

点击此处来配置自动归档存储创建

自动归档存储创建

使用此屏幕可选择 SecurityGateway 自动新建归档存储的频率，何时现有的存储达到一定的存在时间、大小或包含指定数量的邮件。

创建一个新的归档存储...

每年/每季度/每月
如果您希望按每年、每季度或每月自动为域创建一个新的归档存储，请选择以下选项之一。

如果当前归档存储拥有：
如果您希望域的现有存储达到一定大小或包含指定数量的邮件时自动创建新的存档存储，请选择此选项。您可以使用一个或同时使用这两个选项。当同时使用这两个选项时，只要满足任何一个条件，就会创建一个新的存储。

[xx]或更多邮件
选中此框后，只要现有存储中包含指定数量的邮件，就会为该域创建一个新的归档存储。默认值为 5 百万封邮件。

[xx]或更多 GB 大小
选中此框并指定在为该域创建新存储之前，归档存储可以达到多少 GB。

SecurityGateway 每隔几分钟检查一次是否需要创建新的归档存储。归档存储可能会稍微超过在此处配置的阈值。

数据库

使用本地的 Firebird 数据库文件
默认情况下，SecurityGateway 使用本地的 Firebird 数据库文件进行归档。

连接到 Firebird 数据库服务器实例
如果您希望连接到外部的 Firebird 数据库服务器进行归档，请选择此选项。如果您正在使用集群，请选择此项。

使用与 SecurityGateway 数据库相同的服务器
这是您在选择*"连接到 Firebird 数据库服务器实例"*时的默认设置。对于归档，SecurityGateway 将连接到您为处理 SecurityGateway 数据库而设置的同一 Firebird 数据库服务器，并且它将使用相同的凭证。您将需要提供的唯一其他信息是*"数据库路径/别名"*（见下），用于自动创建的归档存储的数据库文件。

连接到这个 Firebird 数据库服务器实例
如果您希望连接到其他 Firebird 数据库服务器来管理数据库，请选择此选项。您将需要提供*服务器名称或 IP*、*端口*、*用户名*和*密码*来连接到该服务器。您还需为所用的数据库文件输入*"数据库路径/别名"*，用于自动创建的归档存储。

数据库路径/别名：
输入将用于为归档存储自动创建的数据库文件的路径。**请注意：**此路径是相对于 Firebird 数据库服务器的，不一定是网络路径。例如 C:\Databases\Archives\$DOMAIN$.fbd。

归档名称宏
您可以在归档的文件名中使用以下宏，以便每个归档在自动创建时可以具有唯一的名称：$DOMAIN$、$YEAR$、$MONTH$ 和 $QUARTER$。例如，将 "C:\Databases\Archives\$DOMAIN$-$MONTH$.fbd"用于*"数据库路径"*将创建一个名为 "Example.com-September.fbd"的数据库文件。此外您必须确保 Firebird 服务器上存在 "C:\Databases\Archives\"文件夹，因为 Firebird 服务器不会动态地自动创建它。

在创建新数据库时，Firebird 服务器不支持动态创建新文件夹。因此如果您希望在*"数据库路径"*中为文件夹名称使用宏，那么您必须首先在 Firebird 服务器上手动创建匹配的文件夹。例如，如果您将*"数据库路径"*设置成 "C:\Databases\Archives\$Domain$\archive.fbd"，那么您必须在 Firebird 服务器上的 "C:\Databases\Archives\"文件夹下，为每个域手动创建子文件夹。因此，我们建议在存档数据库文件名而不是文件夹名中使用宏。

存储位置

为数据库、邮件内容和搜索索引使用不同的目录
默认情况下，归档存储的数据包含在下方"目录"选项中指定的文件夹中，带有两

个子文件夹：\data\ 和 \index\ 文件夹。如果您希望自定义所有三个文件夹的位置，请点击此复选框。

当您选中上方的选项来 *"连接到 Firebird 数据库服务器实例"*，此项仅控制邮件内容和搜索索引的存储位置。将在上方的 *"数据库路径/别名"*选项中指定数据库位置。

目录：
自动创建的归档存储的数据库文件夹的默认位置是：

..\SecurityGateway\Archive\$DOMAIN$\

该路径中的 $DOMAIN$ 宏被转换成与归档存储相关联的域名，此外该文件夹包含 ARCHIVE.FBD Firebird 数据库，其中包含与已归档邮件相关的元数据（域、用户和日期等）。如果没有此文件，将无法还原已归档的数据。该文件夹还拥有 ".\data"和 ".\index"子文件夹来存储已归档的内容和索引。

在您使用集群并已选中上方的选项来 *"连接到 Firebird 数据库服务器实例"*，此项仅控制 ".\data"和 ".\index"这两个子文件夹的位置，而不是数据库文件的位置。将在上方的 *"数据库路径/别名"*选项中指定数据库位置。此外，此处指定的 *"目录"*必须位于网络可访问的位置，并且必须使用 UNC 文件路径。

例如：\\share01\databases\Archive\$Domain$\

在您启用上方的 *"使用不同的目录..."*这个选项时，将使用以下位置：

数据库目录：
这是归档数据库文件的位置。**注意：**如果您选中上方的选项来 *"连接到 Firebird 数据库服务器实例"*，此项将不可用。将在上方的 *"数据库路径/别名"*选项中指定数据库位置。

数据库目录的默认位置是：".\SecurityGateway\Archive\$DOMAIN$\"

内容目录：
自动创建的归档存储的内容文件夹的默认位置是：

..\SecurityGateway\Archive\$DOMAIN$\data

该路径中的 $DOMAIN$ 宏被转换成与归档存储相关联的域名，此外 ".\data"子文件夹包含 archive.sgd 文件。该文件包含压缩格式的归档数据。如果没有此文件，将无法还原已归档的数据。

注意：如果您正在使用集群或已选中上方的选项来 *"连接到 Firebird 数据库服务器实例"*，此文件夹必须位于网络可访问的位置，并且您必须使用 UNC

文件路径 (例如:\\share01\databases\Archive\$Domain$\data)。

索引目录:
自动创建的归档存储的索引文件夹的默认位置是:

..\SecurityGateway\Archive\$DOMAIN$\index

该路径中的 $DOMAIN$ 宏被转换成与归档存储相关联的域名。".\index"子文件夹包含由 CLucene 全文索引引擎生成的全文索引。如果全文索引以某种方式被损坏,则可以重新生成它。可以使用 "归档存储 85"屏幕上的 "维护"选项为归档存储重构 "全文索引"。

注意: 如果您正在使用集群 111或已选中上方的选项来 *"连接到 Firebird 数据库服务器实例"*,此文件夹必须位于网络可访问的位置,并且您必须使用 UNC 文件路径 (例如:\\share01\databases\Archive\$Domain$\index)。

点击此处来管理归档存储
点击此链接来切换归档存储 85屏幕来审核和管理您的存储。

例外 - 域

当配置这些设置时,如果您在页面顶部的 *"针对域:"*下拉列表框中选择了特定域,保存设置后,该域将罗列在此处。为相应的域中点击 *"查看/编辑"*链接来查看或编辑其 "归档"设置,或点击 *"重置"*来将域的设置重置回默认的 "全局"值。

3.3.1.1 自动归档存储创建

使用此屏幕可选择 SecurityGateway 自动新建归档存储的频率,何时现有的存储达到一定的存在时间、大小或包含指定数量的邮件。此屏幕可以从 *"点击此处来配置自动归档存储创建"*链接 (位于归档配置 78页面)来抵达此屏幕。

创建一个新的归档存储...

每年/每季度/每月
如果您希望按每年、每季度或每月自动为域创建一个新的归档存储,请选择以下选项之一。

如果当前归档存储拥有:
如果您希望域的现有存储达到一定大小或包含指定数量的邮件时自动创建新的存档存储,请选择此选项。您可以使用一个或同时使用这两个选项。当同时使用这两个选项时,只要满足任何一个条件,就会创建一个新的存储。

[xx]或更多邮件
选中此框后,只要现有存储中包含指定数量的邮件,就会为该域创建一个新的归档存储。默认值为 5 百万封邮件。

[xx]或更多 GB 大小
选中此框并指定在为该域创建新存储之前,归档存储可以达到多少 GB。

SecurityGateway 每隔几分钟检查一次是否需要创建新的归档存储。归档存储可能会稍微超过在此处配置的阈值。

数据库

使用本地的 Firebird 数据库文件
默认情况下，SecurityGateway 使用本地的 Firebird 数据库文件进行归档。

连接到 Firebird 数据库服务器实例
如果您希望连接到外部的 Firebird 数据库服务器进行归档，请选择此选项。如果您正在使用集群，请选择此项。

使用与 SecurityGateway 数据库相同的服务器
这是您在选择 *"连接到 Firebird 数据库服务器实例"*时的默认设置。对于归档，SecurityGateway 将连接到您为处理 SecurityGateway 数据库而设置的同一 Firebird 数据库服务器，并且它将使用相同的凭证。您将需要提供的唯一其他信息是 *"数据库路径/别名"*（见下），用于自动创建的归档存储的数据库文件。

连接到这个 Firebird 数据库服务器实例
如果您希望连接到其他 Firebird 数据库服务器来管理数据库，请选择此选项。您将需要提供*服务器名称或 IP*、*端口*、*用户名*和*密码*来连接到该服务器。您还需为所用的数据库文件输入 *"数据库路径/别名"*，用于自动创建的归档存储。

数据库路径/别名：
输入将用于为归档存储自动创建的数据库文件的路径。**请注意：**此路径是相对于 Firebird 数据库服务器的，不一定是网络路径。例如 C:\Databases\Archives\$DOMAIN$.fbd。

归档名称宏
您可以在归档的文件名中使用以下宏，以便每个归档在自动创建时可以具有唯一的名称：$DOMAIN$、$YEAR$、$MONTH$ 和 $QUARTER$。例如，将 "C:\Databases\Archives\$DOMAIN$-$MONTH$.fbd"用于 *"数据库路径"*将创建一个名为 "example.com-September.fbd"的数据库文件。此外您必须确保 Firebird 服务器上存在 "C:\Databases\Archives\"文件夹，因为 Firebird 服务器不会动态地自动创建它。

在创建新数据库时，Firebird 服务器不支持动态创建新文件夹。因此如果您希望在 *"数据库路径"*中为文件夹名称使用宏，那么您必须首先在 Firebird 服务器上手动创建匹配的文件夹。例如，如果您将 *"数据库路径"*设置成 "C:\Databases\Archives\$Domain$\archive.fbd"，那么您必须在 Firebird 服务器上的 "C:\Databases\Archives\"文件夹下，为每个域手动创建子文件夹。因此，我们建议在存档数据库文件名而不是文件夹名中使用宏。

存储位置

为数据库、邮件内容和搜索索引使用不同的目录
默认情况下，归档存储的数据包含在下方“目录”选项中指定的文件夹中，带有两个子文件夹：\data\ 和 \index\ 文件夹。如果您希望自定义所有三个文件夹的位置，请点击此复选框。

> 当您选中上方的选项来*“连接到 Firebird 数据库服务器实例”*，此项仅控制邮件内容和搜索索引的存储位置。将在上方的*“数据库路径/别名”*选项中指定数据库位置。

目录：
自动创建的归档存储的数据库文件夹的默认位置是：

..\SecurityGateway\Archive\$DOMAIN$\

该路径中的 $DOMAIN$ 宏被转换成与归档存储相关联的域名，此外该文件夹包含 ARCHIVE.FBD Firebird 数据库，其中包含与已归档邮件相关的元数据（域、用户和日期等）。如果没有此文件，将无法还原已归档的数据。该文件夹还拥有“..\data”和“..\index”子文件夹来存储已归档的内容和索引。

> 在您使用集群并已选中上方的选项来*“连接到 Firebird 数据库服务器实例”*，此项仅控制“..\data”和“..\index”这两个子文件夹的位置，而不是数据库文件的位置。将在上方的*“数据库路径/别名”*选项中指定数据库位置。此外，此处指定的*“目录”*必须位于网络可访问的位置，并且必须使用 UNC 文件路径。
>
> 例如：\\share01\databases\Archive\$Domain$\

在您启用上方的*“使用不同的目录...”*这个选项时，将使用以下位置：

数据库目录：
这是归档数据库文件的位置。**注意：**如果您选中上方的选项来*“连接到 Firebird 数据库服务器实例”*，此项将不可用。将在上方的*“数据库路径/别名”*选项中指定数据库位置。

数据库目录的默认位置是：".."..\SecurityGateway\Archive\$DOMAIN$\"

内容目录：
自动创建的归档存储的内容文件夹的默认位置是：

..\SecurityGateway\Archive\$DOMAIN$\data

该路径中的 $DOMAIN$ 宏被转换成与归档存储相关联的域名，此外“..\data”子文件夹包含 archive.sgd 文件。该文件包含压缩格式的归档数据。如果没有此文件，将无法还原已归档的数据。

注意：如果您正在使用集群[111]或已选中上方的选项来*"连接到 Firebird 数据库服务器实例"*，此文件夹必须位于网络可访问的位置，并且您必须使用 UNC 文件路径（例如：\\share01\databases\Archive\$Domain$\data）。

索引目录：
自动创建的归档存储的索引文件夹的默认位置是：

..\SecurityGateway\Archive\$DOMAIN$\index

该路径中的 $DOMAIN$ 宏被转换成与归档存储相关联的域名。".\index"子文件夹包含由 CLucene 全文索引引擎生成的全文索引。如果全文索引以某种方式被损坏，则可以重新生成它。可以使用"归档存储[85]"屏幕上的"维护"选项为归档存储重构"全文索引"。

注意：如果您正在使用集群[111]或已选中上方的选项来*"连接到 Firebird 数据库服务器实例"*，此文件夹必须位于网络可访问的位置，并且您必须使用 UNC 文件路径（例如：\\share01\databases\Archive\$Domain$\index）。

3.3.2 归档存储

此页面用来管理包含已归档电子邮件的所有归档存储。每个归档存储只能与一个域关联，但您可以将多个存储关联到同一个域，不过每次只有一个存储处于*活动*状态。您可以使用此页上的选项手动创建存储，或者使用归档配置[78]页面上的选项来自动创建归档存储。

"归档存储"页面每行列出一个条目，并且可以通过点击存储列表上方的相应按钮来隐藏或显示各种列。

页面顶部的工具栏包含以下这些选项：

新建
点击*"新建"*来打开"新建归档存储"屏幕，用来手动创建一个新的归档存储。该屏幕等同于编辑归档存储[86]屏幕。

编辑
使用工具栏上的"编辑"按钮，来打开当前列表中与选中条目相应的编辑归档存储[86]屏幕。此外，您还可通过双击一个条目来打开该屏幕。

删除
要删除一个或多个归档存储，从列表中选中条目然后点击*"删除"*。会打开一个对话框询问您是否确定要删除这些存储。您可以使用 Ctrl 和 Shift 键来选择多个条目。

维护
如果您希望为一个或多个归档存储重构全文索引（用于搜索已归档邮件[88]），请选择归档存储并点击**"维护"**和**"重构全文索引"**。系统将要求您确认重构索引的决定，因为在重构进程结束之前，您将无法搜索存档。

针对域：
使用*"针对域："*下拉列表框用于选择要在列表中显示哪个域的归档，或者您可以选择"-全部 -"来显示所有这些归档。默认情况下显示所有归档存储。

3.3.2.1 编辑归档存储

在归档存储[85]屏幕上选择一个归档存储并点击 "编辑"来管理这个对话框中的设置。在您选择手动创建归档存储，而不是使用配置[78]屏幕上的自动创建选项时，就会使用这个屏幕。

归档存储

对这个归档存储启用查询
如果您希望允许使用位于搜索已归档邮件[88]屏幕上的工具来搜索这个归档存储，请勾选此框。禁用时，没有搜索查询会返回这个归档存储中邮件内的任何结果。默认情况下启用此项。

为此处的域归档新邮件
此选项确定这个归档存储是否是此域处于 *"活动"*状态的归档存储，处于活动状态就意味着将为此域将新归档的邮件添加到这个归档存储中。任何域都可以拥有与此相关联的多个归档存储，不过一次只能有一个处于活动状态。例如：在当前存储达到一定大小时，您可以为此域新建一个归档存储，不过在归档存储列表[85]中仍然使旧的归档存储保持可用状态，那样也可以对其进行搜索。此项确定哪个存储接收新归档的邮件。如果域中存在处于活动状态的归档存储，而您编辑了一个非活动的归档存储并启用了此选项，则它将变为活动的归档存储，而其他存储将禁用此选项。

如果您正在为一个域使用自动归档存储创建[82]，并且为域的活动归档存储禁用了此项，则 SecurityGateway 将在必要时为此域创建一个新的归档存储。如果您不使用自动归档存储功能，并且禁用了此域处于活动状态的归档存储，则对该域的归档将停止。

域
这是与归档存储相关联的域。只有一个域可以链接到一个归档存储。仅当手动创建新的归档存储时才可以选择此选项。对于现有的归档存储，无法更改此域。

名称
使用此项来为归档命名，供您自己参考。

数据库

使用本地的 Firebird 数据库文件
默认情况下，SecurityGateway 使用本地的 Firebird 数据库文件进行归档。

连接到 Firebird 数据库服务器实例
如果您希望连接到外部的 Firebird 数据库服务器进行归档，请选择此选项。如果您正在使用集群[111]，请选择此项。

使用与 SecurityGateway 数据库相同的服务器
这是您在选择 *"连接到 Firebird 数据库服务器实例"*时的默认设置。对于归档，SecurityGateway 将连接到您为处理 SecurityGateway 数据库而设置的同一 Firebird 数据库服务器，并且它将使用相同的凭证。您将需要提供的唯一其他信息是 *"数据库路径/别名"*（见下），用于此归档存储。

连接到这个 Firebird 数据库服务器实例
如果您希望连接到其他 Firebird 数据库服务器来管理数据库，请选择此选项。您将需要提供*服务器名称或 IP*、*端口*、*用户名*和*密码*来连接到该服务器。您还需为所用的数据库文件输入*"数据库路径/别名"*，用于此归档存储。

数据库路径/别名：
输入用于此归档存储的数据库文件的路径。**请注意：**此路径是相对于 Firebird 数据库服务器的，不一定是网络路径。例如：C:\Databases\SecurityGateway\Archive\Example.com\ARCHIVE.FBD。此外，您可以在此处使用*"别名"*而不是文件路径，可以通过编辑 Aliases.conf 文件来为该数据库创建别名。Aliases.conf 位于您 Firebird 服务器安装的根文件夹中。

存储位置

为数据库、邮件内容和搜索索引使用不同的目录
默认情况下，归档存储的数据包含在下方"目录"选项中指定的文件夹中，带有两个子文件夹：\data\ 和 \index\ 文件夹。如果您希望自定义所有三个文件夹的位置，请点击此复选框。

> 当您选中上方的选项来*"连接到 Firebird 数据库服务器实例"*，此项仅控制邮件内容和搜索索引的存储位置。将在上方的*"数据库路径/别名"*选项中指定数据库位置。

方向 (D)：
这个文件夹包含 ARCHIVE.FBD Firebird 数据库，其中包含与已归档邮件相关的元数据（域、用户和日期等）。如果没有此文件，将无法还原已归档的数据。该文件夹还拥有"..\data"和"..\index"子文件夹来存储已归档的内容和索引。

> 在您使用集群并已选中上方的选项来*"连接到 Firebird 数据库服务器实例"*，此项仅控制"..\data"和"..\index"这两个子文件夹的位置，而不是数据库文件的位置。将在上方的*"数据库路径/别名"*选项中指定数据库位置。此外，此处指定的*"目录"*必须位于网络可访问的位置，并且必须使用 UNC 文件路径。
>
> 例如：\\share01\databases\Archive\$Domain$\

在您启用上方的*"使用不同的目录..."*这个选项时，将使用以下位置：

数据库目录：
这是归档数据库文件的位置。**注意：**如果您选中上方的选项来*"连接到 Firebird 数据库服务器实例"*，此项将不可用。在这种情况下，将在上方的*"数据库路径/别名"*选项中指定数据库位置。

数据库目录的默认位置是："..\SecurityGateway\Archive\$DOMAIN$\"

内容目录：
该文件夹包含 archive.sgd 文件，其中包含压缩格式的已归档数据。如果没有此文件，将无法还原已归档的数据。默认情况下，该文件夹为“.\data”，而且是“数据库目录”的子文件夹。

注意：如果您正在使用集群[111]或已选中上方的选项来*“连接到 Firebird 数据库服务器实例”*，此文件夹必须位于网络可访问的位置，并且您必须使用 UNC 文件路径（例如：\\share01\databases\Archive\$Domain$\data）。

索引目录：
默认情况下，这个索引目录是“.\index”，而且是数据库目录的子文件夹。索引目录包含由“Lucene 全文索引”引擎生成的全文索引。如果全文索引以某种方式被损坏，则可以重新生成它。可以使用“归档存储[85]”屏幕上的“维护”选项为归档存储重构“全文索引”。

注意：如果您正在使用集群[111]或已选中上方的选项来*“连接到 Firebird 数据库服务器实例”*，此文件夹必须位于网络可访问的位置，并且您必须使用 UNC 文件路径（例如：\\share01\databases\Archive\$Domain$\index）。

3.3.3 搜索已归档邮件

使用此屏幕来搜索启用查询[86]的任何归档储库中包含的已归档邮件。SecurityGateway 将根据您为搜索设置的参数来搜索所有邮件。您可以使用屏幕顶部的*“选定域：”*选项来选择*“所有”*域或特定域，您可以使用“高级”选项按照主题、邮件正文、日期范围、附件、大小和其他一些属性缩小搜索范围。

此屏幕还包含各种工具，用于查看生成的结果邮件、下载这些邮件、以及将邮件回到到其所属的邮箱。

搜索提示

在搜索中支持“?”和“*”通配符。

将“*”与一部分文本一起使用可查找包含该文本任何变体的所有邮件。例如，搜索“send*”将返回包含“send”、“sender”和“sending”等的邮件。搜索“*example.com”将返回包含任何 @example.com 地址或 example.com 域的邮件，例如：mail.example.com 和 sg.example.com 等。

使用引号来搜索精准的语句。例如，搜索“Frank Thomas”将仅返回包含姓名 Frank Thomas 的邮件。如果没有引号，它将返回包含“frank”、“thomas”、“frank thomas”或“thomas frank”字样的任何邮件。

在文字前使用减号将排除包含该文字的邮件。例如，搜索“-John Smith”将找到包含“Smith”的所有邮件，不过排除也包含“John”的所有邮件。

如果出于某些原因，您需要重构全文索引，您可以使用位于“归档存储[85]”屏幕的“维护”选项。

3.3.4 归档合规

此屏幕包含用于控制归档邮件保留时间的各种设置，用于删除从特定用户（可选）发送的归档邮件的工具，以及用于防止删除任何归档电子邮件的“合法保留”选项，无论在 SecurityGateway 中设置的其他任何设置或用户权限如何都是如此。

数据保留

保留归档邮件至少 [xx] 天
启用此项后，无论其他任何归档设置或用户权限如何，至少这些天内都不能删除已归档的邮件。

自动删除存在时间大于 [xx] 天的归档邮件
启用此项后，归档邮件将在这些天后自动删除，除非设置了其他选项来加以阻止，例如下方的“*合法保留*”选项。

仅删除活动的归档储库中的邮件
默认情况下，“*自动删除已归档邮件...*”这个选项仅适用于活动的归档储库。如果您希望删除所有较旧的已归档邮件（即使是那些处于非活动储库中的邮件），请禁用此选项。

合法保留

启用合法保留
启用此项后，无论是否存在所有其他可能的配置，用户权限或保留期，都不能从归档中删除任何电子邮件。

忘记联系人

使用这些选项可删除从指定电子邮件地址（并可选择发送到）指定电子邮件地址的所有归档邮件。

电子邮件地址：
指定其已归档邮件是您希望删除的电子邮件地址。默认情况下，忘记联系人选项仅删除从“**发件人**”这个地址发送的已归档邮件。如果您也希望删除发往“**收件人**”地址的归档邮件，请启用下方的“*...也删除发往此联系人的所有邮件*”这个选项。

...也删除发往此联系人的所有邮件
如果您希望删除发往“**收件人**”地址而不仅仅是从“**发件人**”地址发出的归档邮件，请勾选此框。

发送告知已删除所有邮件的确认电子邮件
如果您希望 SecurityGateway 在删除所有邮件后发送确认电子邮件，请使用确认电子邮件选项。您可以将此邮件发送给自己，正在删除其归档邮件的联系人，并指定一些其他地址。

请点击此处删除此联系人收发的所有邮件
一旦您将“忘记联系人”选项设置为所需设置后，点击此链接可删除已归档的邮件。

3.3.5 导出

使用此页面上的选项导出一个域的所有已归档邮件，并将它们压缩成可以下载的 .zip 文件。当 .zip 文件准备就绪时，将向指定的电子邮件地址发送通知，其中包含下载 .zip 文件的链接。

要导出已归档的邮件，请选择一个域，指定您希望接收指向归档的下载链接的电子邮件地址，然后点击 "导出"。

3.4 安全通信

3.4.1 配置

SecurityGateway 新的 "安全通信"功能为您的用户提供了一种向其域外的收件人发送安全邮件的方式，通过这种方式，邮件绝不会离开 SecurityGateway 服务器。它通过使用安全的通信网络门户来实现这一点。发送邮件后，收件人会收到一封电子邮件通知，告知他们有可用的安全邮件，其中包含用于创建安全邮件收件人[91]账户的链接，以便他们可以查看位于您 SecurityGateway 服务器上的邮件。通过收件人的浏览器访问安全邮件，并通过 HTTPS 加密在 SecurityGateway 服务器和收件人之间维护端到端的加密。安全通信需要有效的 SSL 证书[103]并启用 HTTPS[100]（还请参阅：HTTPS 服务器[107]）。收件人可以查看和答复 SecurityGateway 门户中的邮件，并且他们可以选择性地向指定的用户列表编写新的安全邮件[95]。还请参阅：收件人[91]和收件人选项[92]来获取有关安全邮件收件人账户的更多信息。

在使用位置屏蔽[178]来阻止来自特定国家/地区的连接，将无法为该国家/地区的收件人使用安全通信，因为他们将无法连接到SecurityGateway 来查看安全邮件。

发送安全邮件

要使用 "安全通信"系统而不是使用传统的邮件投递来发送邮件，请创建内容过滤器[199]或数据泄露过滤器[190]规则，这些规则使用 *"发送为安全网络邮件"*操作。例如，您可以创建一个规则，该规则会在主题以 "[Secure Message]"开头时，将邮件作为安全邮件发送。或者，您可以手动创建一个 Sieve 脚本来发送安全邮件，该脚本使用 Sieve 操作[227]：vnd.mdaemon.securewebmsg。

启用安全通信

勾选此框来启用 "安全通信"系统。

自动创建安全通信收件人
默认情况下，每当向某人发送安全邮件时，将为他们创建一个安全邮件收件人[91]账户，并为他们提供一个链接来访问该账户并查看邮件。如果您希望手动创建所有收件人账户，请禁用此选项。

如果禁用此选项，则必须先在收件人[91]页面上手动创建安全邮件收件人，以便他们能够接收安全邮件。如果规则或脚本指示应发送

安全邮件，但其收件人未知，则会将该邮件退回给发件人。

例外 - 域

当配置这些设置时，如果您在页面顶部的 *"针对域："* 下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。请点击相应域的 *"查看/编辑"* 链接以查看或编辑其 "安全通信"设置，或点击 *"重置"* 将域设置重置为默认全局值。

3.4.2 收件人

此页面包含每个 "安全邮件收件人"账户的条目，这些账户将被自动[90]或手动创建。如果您希望手动创建新的收件人账户，请点击工具栏上的 **"新建"**。您可以通过选中或取消选中 "已启用"列中相应的复选框来快速启用或禁用账户。要查看或编辑账户的属性，例如其电子邮件地址、姓名和密码，请双击该账户（或选择它并点击 **"编辑"**）。要编辑其归档、语言和每页显示的项目设置，请选择该账户并点击 **"设置[92]"**。要查看收件人账户的邮件日志[38]，请选择该账户并点击 **"邮件"**。

在使用位置屏蔽[178]来阻止来自特定国家/地区的连接，将无法为该国家/地区的收件人使用安全通信，因为他们将无法连接到SecurityGateway 来查看安全邮件。

创建或编辑收件人账户

如果您希望手动创建新的收件人账户，请点击工具栏上的 **"新建"**。要编辑账户，请选择它并点击 **"编辑"**。

属性

该账户被禁用
如果要禁用收件人账户，可点击该复选框。

相关联的本地域：
选择您希望与账户关联的域。对于自动创建的收件人账户，会将其设置为安全邮件发件人的域。如果您已使用 *"域："* 下拉列表（位于收件人选项[92]页面，来为此域指定自定义选项，则这些选项将用于收件人账户而不是全局选项。此外，每当收件人访问它来查看安全邮件时，安全 web 门户将使用关联域的贴牌和自定义图像[110]。此外，域管理员将只能看到与他们有权访问的域相关联的收件人账户。最后请注意，如果来自多个本地域的用户发送相同的收件人安全邮件，则收件人将为每个关联的本地域拥有一个单独的收件人账户。

电子邮件地址
这是收件人账户的电子邮件地址，用于登录 SecurityGateway 的安全邮件 Web 门户。

真实姓名
使用此空格来输入收件人的姓名。对于自动创建的账户，如果在已发送的安全邮件的 "收件人"报头中包含姓名，则会自动填写。

收件人将收到一个邀请以指定他们自己的密码
在创建安全邮件收件人账户时，如果您希望收件人收到一封电子邮件，其中包含指向关联域的 Web 门户的链接，将提示他们为其账户创建密码，请选择此选项。在账户使用此选项后，它会自动切换到下方的 *"为收件人指定密码"*。如果您切换回此选项，它将再次发送电子邮件。

需要 PIN 来进行账户设置
如果您希望收件人在创建密码时输入 PIN，请点击此框并输入六位数字 PIN。

此 PIN 不会包含在发给收件人的邀请电子邮件中。应通过电子邮件以外的方法（例如电话）将其传达给收件人。

为收件人指定密码
如果您希望手动输入收件人账户的密码，请在此处进行。有新密码都必须包含至少八个字符，并且至少包含以下各项之一：

- 大写字符
- 小写字符
- 数字
- 特殊字符，例如. ;,_.?/-=

设置

选择一个收件人并点击工具栏上的 **"设置"**来为收件人账户编辑下方的选项。

选项

不为该账户归档邮件
此选项将阻止此收件人账户收发的安全邮件被归档。

为此账户删除所有已归档的邮件
点击此链接可删除已为此收件人账户归档的所有邮件。

语言：
将以此语言发送系统生成的电子邮件。用户可以在安全邮件 Web 门户中自行更改此设置。使用位于收件人选项 92 页面上具有相同名称的选项来设置默认值。

每页显示的项目数：
这是每页将显示给 Web 门户中的收件人的邮件数。收件人账户可以在 Web 门户中为自己设置选项。使用位于收件人选项 92 页面上具有相同名称的选项来设置默认值。

3.4.3 收件人选项

使用此页面来配置将应用于安全邮件收件人账户的各种选项和默认设置，并指定他们将能在 Web 门户中为自己配置的选项。

下方的“丢失密码”、“显示密码”和“记住设备”选项控制它们的相应要素是否会出现在安全邮件门户登录页面上。不过，这些选项取决于收件人通过适当的 URL 到达门户：<SG BASE URL>/SecurityGateway.dll?view=login_ex. 例如："https://sg.company.test:4443/securitygateway.dll?view=login_ex"。这是在创建发送给收件人以设置其账户的链接时使用的 URL。作为安全邮件收件人登录，会设置一个 cookie，以便在用户导航到 SecurityGateway 的基本 URL 时（例如不含“view=login_ex”），他或她仍将被重定向到安全邮件门户。如果用户导航到不存在 cookie 的机器上的基本 URL，他或她仍然可以登录，但这些登录页面元素将受位于以下位置的等效选项控制：设置 » 账户 » 用户选项[60]。为此，请确保为安全邮件收件人发布的任何 URL 都包含适当的“/SecurityGateway.dll?view=login_ex”结尾。

访问控制

允许收件人修改其密码
通常，允许收件人账户在安全邮件门户网站中更改其密码。如果您不希望允许他们这么做，请清除该复选框。

显示密码字段的“显示密码”图标
每个密码字段均包含一个眼睛图标，收件人可以点击该图标来查看他刚在该字段中键入的密码。如果您不想让收件人账户看到他们的密码，请禁用此选项。

允许收件人启用“双重验证”
“双重验证”是额外的安全层，要求您在登录时输入密码和手机上身份验证应用程序生成的特殊安全代码。如果您希望允许安全邮件收件人将其账户配置为在登录安全邮件门户网站时需要双重身份验证，请勾选此框。启用后，收件人使用安全 HTTPS 连接从浏览器登录，双重验证[29]选项将在“账户设置”页面上可用，以便收件人可以根据自己的选择进行设置。

要求用户启用“双重验证”
如果您希望所有安全邮件收件人在登录时使用“双重验证”，请选中此框。启用此选项后，收件人首次登录时将看到设置“双重验证”的页面。

允许每台设备记住收件人（需要 HTTPS）
启用此项时，每当收件人通过安全的 HTTPS 连接进行连接时，将在“安全邮件门户登录”页面上显示*“在此设备上记住我”*这个选项。如果收件人选中了该框，则从那时起，只要在完成操作后仅关闭浏览器而不使用“注销”选项，并且在同一设备上访问该门户，他就会自动登录。如果他退出，那么下次连接时他将必须再次登录。收件人被记住的天数将在下方的*“天数...”*选项中指定。之后将要求他再次登录。默认情况下禁用此项。**注意：**只要“记住我”选项在当前设备或浏览器上处于活动状态，“安全通信”用户就可以使用*“在该设备/浏览器上不记住我”*这个选项、他们可以点击该链接取消在设备上“记住我”。

将记住收件人的天数（从 1 到 365）
在使用*“允许按设备记住收件人”*这个选项时，这是在需要再次登录之前将记住收件人的天数。默认情况下将此值设置成 30。

登录选项

在登录屏幕上显示“忘记密码”链接
默认情况下，“忘记密码”链接出现在安全邮件门户的登录页面上，可用于通过电子邮件将链接发送给收件人以更改其密码。如果您不希望在登录页面上显示“忘记密码”链接，请清除此复选框。

在登录屏幕上显示以下管理员联系信息
如果您希望在登录页面上包含一些管理员的联系信息或链接，请激活此项并在框中输入一些文本。您在框中输入的文本可以包含一些 HTML，如锚点和图像。

默认值

语言：
使用此下拉列表来设置服务器在将系统生成的邮件发送给安全邮件收件人时将使用的默认语言。您可以使用相应的选项为特定用户设置此选项。在收件人 91 页面上选择一个收件人，然后点击工具栏上的设置以访问该选项。收件人还能在安全邮件门户的“账户设置”页面上为自己覆盖此设置。

对照来自第三方服务的已泄露密码列表检查密码
SecurityGateway 可以对照来自第三方服务的已泄露密码列表来检查收件人的密码，并且无需将密码传输到该服务即可执行此操作。如果收件人的密码出现在列表中，并不表示该账户已被黑客入侵。而是意味着某人在某处使用了与他们的密码相同的字符，并且发生了数据泄露事件。从未在其他任何位置使用过的唯一密码更加安全，因为黑客在字典攻击中可能会使用已公开的密码。请参阅Pwned Passwords（已泄露密码）获取更多信息。

使用下拉列表框来选择自上次检查密码以来，您希望多久对列表进行一次密码检查。您可以选择：

- 从不（不对照该列表检查密码。这是默认设置。）
- 自上次检查以来的一天
- 自上次检查以来的一周
- 自上次检查以来的一月

每页显示的项目数
这是每页将显示给 Web 门户中的收件人账户的默认邮件数。要为特定的收件人账户设置此选项，请在收件人 91 页面上选择收件人，然后点击工具栏上的“设置”来访问该选项。收件人账户可在 Web 门户中为自己设置选项。

使用条款

要求收件人在登录之前接受以下使用条款
如果您希望每次登录安全邮件门户时都要求收件人接受文本内容，例如使用条款声明，请启用此选项并在框中输入文本。收件人可以通过勾选一个框来接受该声明。

新建收件人

创建安全邮件收件人时向全局管理员发送警报
每当创建新的安全邮件收件人账户时，如果您希望向全局管理员[50]发送警报，请勾选此框。

对照第 3 方泄露的密码列表检查新收件人的密码
在默认情况下，每个新收件人的初始密码都会对照上方列出的已泄露密码列表进行检查，这在上述 *"对照已泄露的密码列表检查密码..."*选项中概述过。如果您不希望对照列表检查新的收件人账户密码，请清除此复选框。

例外 - 域

当配置这些设置时，如果您在页面顶部的 *"针对域："*下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。请点击相应域的 *"查看/编辑"*链接以查看或编辑其 "安全通信"设置，或点击 *"重置"*将域设置重置为默认全局值。

3.4.4 邮件编写

这是一个特定于域的设置，您可以使用它来允许与所选域相关联的安全邮件收件人账户，以便从预定列表向本地用户编写新邮件。收件人将从安全邮件门户中编写邮件，并从下拉列表选择 **"收件人"**地址。**注意：**始终允许收件人账户答复他们收到的任何安全邮件。

新建邮件编写

允许安全邮件收件人向指定的本地用户编写新邮件
请从 *"域："*列表选择一个域，并勾选此框，以便允许与该域相关联的[91]收件人账户来编写新邮件。然后，这些账户将能够向您添加到下面的 "选定地址"列表中的任何本地地址编写邮件。如果您不希望允许域的收件人账户编写新邮件，请取消选中该框。他们将只能答复他们收到的安全邮件。

可用地址：
此框列出所选域的用户。选择一个地址并点击向右箭头，将其移至 "选定地址"框。

选定地址：
这些是与所选域关联的安全邮件收件人账户，可以向其发送新邮件的本地地址。

3.5 免责声明（报头/脚注）

该页面用来管理您所有的邮件免责声明。邮件免责声明是服务器可以动态添加到入站、出站和本地邮件正文上方或下方的文本部分。管理员可以使用标记免责声明[96]屏幕来创建免责声明模板，可以使用纯文本、标准 HTML 和自定义 SecurityGateway 标记中的任意一种。免责声明模板适用于 HTML 正文和邮件文本正文，而且此模板可以指定给特定域或者供全局应用。将为各个免责声明创建 Sieve 脚本[219]，将模板链接到所需的触发器。还可以直接在 Sieve 脚本页面创建这些 sieve 脚本。

邮件免责声明页面每行列出一个条目且有七列：启用、描述、类型、入站、出站、内部、域。要了解这些项目的详细信息以及如何创建和编辑免责声明，请参见编辑免责声明[96]屏幕

页面顶部的工具栏包含了以下四个选项：

新建
点击 *"新建"*来打开新建免责声明屏幕，用来创建新的邮件免责声明。该屏幕等同于 "编辑免责声明"屏幕。

编辑
使用工具栏上的编辑按钮，以打开目前列表中选中条目的相应 "编辑免责声明[96]"屏幕。此外，您还可通过双击一个条目来打开该屏幕。

删除
要删除一条或多条免责声明，从列表中选中条目然后点击 *"删除"*。会打开一个对话框询问您是否确定要删除这些免责声明。您可以使用 Ctrl和 Shift 键来选择多个条目。

针对域：
使用 *"针对域："*下拉列表选择框以选择该列表中所显示的域免责声明，或者您可以选择 "- 全局 --"仅显示全局免责声明。默认情况下会显示所有的免责声明，不管是全局还是特定域。

3.5.1 与列表中当前选定条目相应的编辑免责声明

使用 *"新建"*或 *"编辑"*选项（位于邮件免责声明[95]页面）来打开 "编辑免责声明"屏幕用来创建或编辑您的邮件免责声明模板。在此屏幕上，您可以启用或禁用免责声明，将其与特定域关联，指定其类型（页眉，页脚或自定义），并指定使用该类型的邮件类型：入站、出站或本地邮件。

该免责声明被禁用
如果您希望禁用这个免责声明，可点击此复选框。它仍然将在邮件免责声明[95]列表中显示，不过 SecurityGateway 不再将其添加到任何邮件。清除复选框以再次使用它。

该免责声明用于此域：
使用下拉列表指定 SecurityGateway 域与此免责声明相关联，或选择 *"全局"*来将其与所有域关联。

描述

描述
使用该区域为免责声明提供姓名或说明。这仅供您参考，并出现在免责声明列表中。

类型

此项用来指定免责声明的类型：页眉、页脚或自定义。

页眉
如果您希望将免责声明添加到邮件顶部，位于邮件正文上方，请选择 *"页眉"*。

页脚
如果您希望将免责声明添加到邮件底部，位于邮件正文下方，请选择*"页脚"*。

自定义
如果您希望使用下面列出的特定 SecurityGateway 标签创建自定义免责声明，请选择*"自定义"*。使用自定义免责声明，您可以在正文上方和下方添加文字。所有自定义免责声明都需要"<sg:ORIGINAL_BODY>"标签。

规则

此选项用于指定应该添加免责声明的邮件类型。

给入站邮件添加免责声明
如果您希望将免责声明添加到发往以上选定域的所有入站邮件，请选择此选项。如果您已将此指定为全局免责声明，则它将被添加到所有入站邮件，而不管域名如何。

给出站邮件添加免责声明
如果您希望将免责声明添加到上述所选域中的所有出站邮件，请选择此选项。如果您已将此指定为全局免责声明，则它将被添加到所有发出的邮件中，而不管发送者是谁。

给本地邮件添加免责声明
如果您希望将免责声明添加到以上选择的域中和来自上面所选域的任何邮件，请选择此选项。例如，一封邮件从 frank@example.com 发往 hmudd@example.com 并添加了免责声明，不过从 frank@example.com 发往 biff@example.net 的邮件则不添加免责声明。如果您已将此指定为全局免责声明，则会将其添加到每个域的本地邮件。

文本

这是您指定免责声明模板内容的地方，并将模板指定为纯文本或 HTML。纯文本模板只能包含文本，但 HTML 模板可以包含 HTML 代码和下面列出的特殊 SecurityGateway 标签。

纯文本（将编译 HTML 字符）
纯文本免责声明是默认选项。启用此选项时，无论文本中是否存在任何 HTML 代码，只有纯文本将被添加到邮件中。任何 HTML 标签或字符都将被编码为纯文本并添加。"My Disclaimer"文本将按原样插入，包括 HTML 标签，而不是转换为粗体文本或删除 HTML 标签。因此，如果您创建纯文本模板，请不要包含任何 HTML 代码。

当您将免责声明类型指定为*"自定义"*时，纯文本模板可以包含"<sg:ORIGINAL_BODY>"标签，允许您将邮件正文放在模板的任何位置。所有其他标记或 HTML 字符将仅显示为纯文本而不是作为代码处理。

以下是纯文本页眉模板的示例：

```
---------------------------------------------
The views in this message are not necessarily
those of example.com or its affiliates.
---------------------------------------------
```

以下是纯文本自定义模板的示例：

```
The following message was sent by an employee
of example.com.
--
<sg:ORIGINAL_BODY Field="body:all">{Original Email}
</sg:ORIGINAL_BODY>
-----------------------------------------------
The views in this message are not necessarily
those of example.com or its affiliates.
-----------------------------------------------
```

HTML 模板

如果你想创建一个 HTML 免责声明模板，请禁用 *"纯文本"*选项。HTML 模板可以包含 HTML 代码和下面列出的特殊 SecurityGateway 标签。

HTML 报头模板的示例如下：

```
<HTML><HEAD>
<style type="text/css">
.blueboldtext { font-family: Geneva, fixed-width; font-size: 13;
color: #114477; font-weight: bold; }
</style></HEAD>
<BODY>
<DIV>This is my header text!</DIV>
<sg:HTML_ONLY><span class="blueboldtext">Only show this text in the
HTML body!</span></sg:HTML_ONLY>
<sg:TEXT_ONLY>Only show this text in the Plain Text
body!</sg:TEXT_ONLY>
<BR>
-------------<br />
</BODY></HTML>
```

自定义 HTML 模板的示例如下：

```
<DIV> </DIV>
<DIV>This is my header text!</DIV>
<br />---------</DIV>
<sg:ORIGINAL_BODY Field="body:all">{Original Email}
</sg:ORIGINAL_BODY>
<br />---------</DIV>
<DIV>This is my footer text!</DIV>
<DIV> </DIV>
<DIV>This text will be in html and text body<br />
<sg:HTML_ONLY>Only show this text in HTML message!</sg:HTML_ONLY>
<sg:TEXT_ONLY>Only show this text in Plain Text
message!</sg:TEXT_ONLY></DIV>
```

您不需要将 HTML、HEAD 或 BODY 标签添加到免责声明模板中。如果您确实添加了它们，则标签将与每封电子邮件中的相应标签合并。

SecurityGateway 标签

您可以在免责声明模板中使用三种自定义 SecurityGateway 标签。无论模板类型如何，所有这三个标签都可以在 HTML 模板中使用。自定义类型纯文本模板只能使用“sg:ORIGINAL_BODY>”标签。

<sg:ORIGINAL_BODY></sg:ORIGINAL_BODY>
该标签在模板中表示放置原始正文的位置。当您将免责声明指定为页眉或页脚时，标签将自动放置在适当的位置。对于自定义类型免责声明，您必须手动将此标签放置在希望显示邮件正文的位置。对于自定义 Sieve 脚本 219，它可以放置在任何地方，但必须存在。

此标签可用于任何类型的 HTML 免责声明模板：页眉、页脚或自定义。无论选择何种类型，邮件的正文总是会出现在该标签指定的位置。对于纯文本模板，只能在自定义类型免责声明中使用。

<sg:HTML_ONLY></sg:HTML_ONLY>
任何放置在这个标签内的东西只会出现在邮件的 HTML 正文中；它不会出现在文本正文中。此标签可用于*纯文本*免责声明模板。

<sg:TEXT_ONLY></sg:TEXT_ONLY>
任何放置在这个标签内的东西只会出现在邮件的文本正文中；它不会出现在 HTML 正文中。此标签可用于*纯文本*免责声明模板。

Sieve 脚本

如果您想添加用户定义的自定义免责声明，请使用 Sieve 脚本 219。触发免责声明的条件与任何其他 sieve 脚本相同。在使用 sieve 编辑器时，模板中的某些字符需要转义。以下 sieve 过滤器作为用户定义的免责声明的示例提供：

```
require ["securitygateway","body"];

if allof(body :text :contains "Make money now!")
{
disclaimer "text:
<HTML xmlns:sg = \"http://www.altn.com/Products/SecurityGateway-
Email-Firewall/\">
<HEAD><META http-equiv=\"Content-Type\" content=\"text/html;
charset=UTF-8\" />
</HEAD>
<BODY>
<DIV>This is my header text!</DIV>
<DIV>Another line of header text!</DIV>
<DIV> </DIV>
<DIV>---------<br />
<sg:ORIGINAL_BODY Field=\"body:all\">{Original Email}
</sg:ORIGINAL_BODY>
<br />---------</DIV>
<DIV> </DIV>
<DIV>This is my footer text!</DIV>
<DIV>Another line of footer text!</DIV>
```

```
<DIV> </DIV>
<DIV>This text will be in html and text body<br />
<sg:HTML_ONLY>Only show the image and this text in HTML
message!</sg:HTML_ONLY>
<sg:TEXT_ONLY>Only show this text in Plain Text
message!</sg:TEXT_ONLY></DIV>
</BODY></HTML> ."
; }
```

3.6 系统

"*设置/用户*"菜单下的系统部分包含下列系统相关功能的链接：

加密 100—此页面用于配置 SecurityGateway 的各种加密设置。SecurityGateway 支持带 STARTTLS SMTP 扩展的安全套接字层 (SSL) 协议，以防止他人截获并阅读您的电子邮件。它还支持 HTTPS，从而为 web 接口提供了同样的保护。

HTTP 服务器 107— "HTTP 服务器"页面用于配置与 SecurityGateway 的 Web 界面相关的各种设置。您可指定在 SecurityGateway 创建的登录链接中使用的主机名，HTTP 和 HTTPS 端口，以及其他相关的 HTTP 设置。

贴牌/定制图像 110—此页面提供用于自定义显示在登录页面和导航侧栏上的横幅图像的选项。

目录 109—该页列出了 SecurityGateway 用来管理各类文件的文件夹。通过更改该页上的任意路径，可定制文件夹位置。

磁盘空间 110—磁盘空间页用于配置 SecurityGateway 来监控可用磁盘空间。它包含的选项可用于向管理员发送警告邮件，并/或在磁盘空间不足时停止接收邮件。

查看配置 111—该页显示当前所有 SecurityGateway 设置。当试图为 SecurityGateway 服务器诊断故障或寻求技术支持时，该功能会很有用。该页包括将当前配置保存为 XML 文件的选项。

3.6.1 加密

SecurityGateway 合并了最新的加密技术来保护您的数据。安全套接层 (SSL)协议—也叫做传输层安全 (TLS)— 通过使用 STARTTLS SMTP 扩展名来防止其他人拦截和读取您的邮件。SecurityGateway 中的 HTTPS 为 web 界面提供了相同的保护。

由 Netscape 通信公司所研发的 SSL 协议是用来保证服务器/客户端进行互联网通信的标准方式。它提供了服务器验证、数据加密和用于 TCP/IP 连接的可选客户端验证。此外，因为 SSL 已构建入当前所有主要浏览器，只需在您的服务器上安装一个有效的数字证书，当连接至 SecurityGateway 时，即可激活连接浏览器的 SSL 功能。若您使用邮件客户端连接，在支持 SSL/TLS 后，SecurityGateway 还要支持 STARTTLS SMTP 扩展名。不过，您必

须先将您的客户端配置为会使用 SSL，且其必须支持此扩展名—并非所有邮件客户端都要支持，大部分支持即可。

电子邮件和 HTTPS 加密

启用 SMTP 和 HTTPS 的 SSL 和 STARTTLS 支持
点击此选择框激活 SSL/TLS 协议支持以及 STARTTLS 扩展名，使用下方选则证书框中的"激活"证书。必须启用此选项，而且若您希望使用 HTTPS 登录到 SecurityGateway 的 web 界面，必须激活一个有效的证书。默认情况下，禁用该选项。

尽可能发送带 STARTTLS 的邮件
若您希望 SecurityGateway 为它发送的每一封 SMTP 邮件使用 STARTTLS 扩展名，请点击此选项。若与 SecurityGateway 相连的服务器不支持 STARTTLS，那么邮件将以常规方式投递而不使用 SSL。默认情况下，禁用该选项。

SSL 协商失败将在没有 SSL 的情况下重试一小时
此选项会将在 SMTP 会话期间遇到 SSL 错误的主机临时列入允许列表。该允许列表每小时进行重置。

自动检测并激活更新的证书
启用此选项后，系统将在其夜间维护过程中执行检查。对于每个活动证书，它将检查以查看：系统上是否有另一个证书稍后到期，它是否针对相同的主机名，以及它是否包括所有备用主机名。如果存在这样的证书，系统将自动激活此证书。当系统上有自动更新证书的调度任务时，例如 Let's Encrypt 104，特别有用。默认情况下启用此项。

启用 REQUIRETLS (RFC 8689)
RequireTLS 允许您标记*必须*使用 TLS 发送的邮件。如果无法使用 TLS（或者 TLS 证书交换的参数不可接受），则退回邮件，而不是不安全地投递邮件。有关 RequireTLS 的完整说明，请参阅：RFC 8689: SMTP Require TLS Option.

默认情况下，启用 RequireTLS，但是将受 RequireTLS 进程约束的唯一邮件是被使用新的内容过滤器操作 199，"*为 REQUIRETLS 标记邮件...*"的"内容过滤器"规则特别标记的邮件，或发送至 <local-part>+requiretls@domain.tld (例如 arvel+requiretls@mdaemon.com)的邮件。将所有其他邮件视为已禁用该服务。此外，必须满足几个要求才能使用 RequireTLS 发送邮件。如果它们中的任何一个失败，该邮件将弹回，而不是以明文形式发送。这些要求是：

- 必须启用 RequireTLS。
- 必须通过"内容过滤器"操作或"<localpart>+requiretls@..."地址将该邮件标记为需要 RequireTLS 处理。
- 收件人域的 MX 记录必须由 MTA-STS 验证。
- 指向收件主机的连接必须使用 SSL (STARTTLS)。
- 收件主机的 SSL 证书必须与 MX 主机名匹配，并链接到受信任的 CA。
- 收件邮件服务器必须支持 REQUIRETLS，并在 EHLO 响应中声明。
- 如果这些要求中的任何一个失败，则邮件不会被投递，并退回给发件人。

启用 MTA-STA (RFC 8461)
默认情况下启用 MTA-STS 支持，详细说明请参阅 RFC 8461: SMTP MTA Strict Transport Security (MTA-STS).

SMTP MTA 严格传输安全 (MTA-STS)是一种机制，使邮件服务供应商 (SP)能够声明其接收传输层安全 (TLS)和保护 SMTP 连接的能力，并指定发件 SMTP 服务器是否应拒绝投递给不为 TLS 提供受信任的服务器证书的 MX 主机。

要为您自己的域设置 MTA-STS，您需要创建一个 MTA-STS 策略文件，该文件可以通过 HTTPS 从 URL https://mta-sts.domain.tld/.well-known/mta-sts.txt 下载，其中 "domain.tld"是您的域名。策略文本文件应包含以下格式的几行信息：

```
version: STSv1
mode: testing
mx: mail.domain.tld
max_age: 86400
```

模式可以是 "none"、"testing"或 "enforce"。每个 MX 主机名应有一个 "mx"行。通配符可用于子域，例如 "*.domain.tld"。存在时间最大值以秒为单位。常规值是 86400 (1 天) 和 604800 (1 周)。

还需要 _mta-sts.domain.tld 上的 DNS TXT 记录，其中 "domain.tld"是您的域名。它必须具有以下格式的值：

```
v=STSv1; id=20200206T010101;
```

每次更改策略文件时，都必须更改 "id"的值。通常为这个 id 使用时间戳。

启用 TLS 报告 (RFC 8460)
默认情况下禁用 TLS 报告功能，更多详细信息请参阅RFC 8460: SMTP TLS Reporting.

TLS 报告功能允许使用 MTA-STS 的域收到有关检索 MTA-STS 策略或使用 STARTTLS 协商安全通道的任何失败的通知。启用后，SecurityGateway 会每天向已在当天向其发送 (或尝试发送)邮件的每个启用 STS 的域发送报告。提供了多个选项来配置报告将包含的信息。

要为您的域设置 TLS 报告，请启用 DKIM 签名 155，并在 _smtp._tls.domain.tld 创建一个 DNS TXT 记录，其中 "domain.tld"是您的域名，具有以下格式的值：

```
v=TLSRPTv1; rua=mailto:mailbox@domain.tld
```

其中 mailbox@domain.tld 是您要向其发送域报告的电子邮件地址。

选择证书

要为 SecurityGateway 支持 SSL/TLS 和 HTTPS，您需要 SSL/TLS 证书 103 (见下)。证书是由证书颁发机构 (CA) 104颁发的小型文件，用来验证与其预期的服务器建立连接的客户端或浏览器 并启用 SSL/TLS/HTTPS 来保护与该服务器建立的连接。

此框中列出了您创建的所有 SSL 证书。SecurityGateway 生成的证书是自己签名的，这就表示该证书的发行人，或者说证书颁发机构 (CA)，与证书的拥有者是同一人。该证书当然有效且允许，不过有可能每当用户连接至 SecurityGateway 的 HTTPS URL 时，有一些用户就会被问道是否希望进入站点并/或安装该证书。因为该 CA 并未列于它们所信

赖的 CA 列表中。当用户同意安装证书并信任您的 SecurityGateway 域作为有效 CA 时，在连接时他们将不再看到安全警告邮件。他们是否要通过一切步骤取决于他们所使用的浏览器，他们所放置的安全性限制，等等。

创建并删除 SSL 证书
要创建一个新证书，点击选择证书框顶部工具栏上的*新建*。将会打开 SSL 证书 103 屏幕（见下）。欲删除一个现有证书，选中该证书然后点击*"删除"*。

激活一个 SSL 证书
要激活 SSL 证书，请点击该证书的*激活*选框并点击**保存**。

配置 Let's Encrypt
如果您正在使用 Let's Encrypt 作为您的 CA 来自动化证书管理，请点击**配置 Let's Encrypt**来打开 Let's Encrypt PowerShell 更新 106 页面，这将帮助您轻松地配置并运行所需的 PowerShell 脚本，包含在 "SecurityGateway\LetsEncrypt"文件夹。要了解更多信息。请参阅下方的使用 Let's Encrypt 来管理您的证书 104。

STARTTLS 允许列表

使用此选项可指定您希望从 STARTTLS 免除的任何 IP 地址、主机或域。发送到列出的任何条目时，STARTTLS 将永远不会使用，并且 STARTTLS 从不被通告给列表上的任何连接主机或 IP。

STARTTLS 请求列表

在 STARTTLS 请求列表中的主机或 IP 地址的 SMTP 连接必须使用 STARTTLS。如果 STARTTLS 不可用或失败，则不会发送该消息。

SSL 证书

该屏幕用于创建新的 SSL 证书。欲创建一个新证书，点击*"加密"*页面上选择证书工具栏中的"新建 100"，然后输入您的证书信息。完成后，点击*"保存并关闭"*来创建证书。

创建证书

主机名
输入您的用户将会连接的主机名称（例如，"mail.example.com"）。

机构/公司名
在此输入"拥有"此证书的机构或公司。

替换主机名（用逗号分隔多个项目）
SecurityGateway 不支持为各个域服务的分离证书—所有域必须共享一个单一的证书。若用户可能连接的主机名存在着替换主机名，并且您希望该证书同样适用于那些名称，那么请在此输入这些域名，并以逗号隔开。允许通配符，例如"*.example.com"。

加密密钥长度
为此证书选择所需位长度的加密密钥。加密密钥的位数越长，已传输的数据也将越安全。不过请注意，并非所有的应用程序都支持大于 512 的密钥长度。

国家/地区
选择您的服务器所在国家或地区。

使用第三方 CA 颁发的证书

如果您从 SecurityGateway 以外的其他渠道购买或者生成了证书，则通过使用 Microsoft 管理控制台将其导入 SecurityGateway 所用证书库，您仍可使用该证书。一旦证书被导入到 Windows 中，它应该出现在 SecurityGateway 中，以便它可以被使用。要导入证书：

1. 在 Windows 工具栏上，点击 "开始 » 运行..."，然后在文本框中输入 "mmc /a"。
2. 点击 "确定"或按 "回车"。
3. 在 Microsoft 管理控制台中，点击菜单栏上的 "文件 » 添加/删除管理单元..."，（或在键盘上按下 "Ctrl+M"）。
4. 在 "*添加或删除管理单元*" 对话框上，点击 "证书"，然后点击 "添加"。
5. 在 "*证书管理单元*"对话框上，选择 "计算机账户"，然后点击 "下一步"。
6. 在 "*选择计算机*"对话框上，选择 "本地计算机"，然后点击 "完成h"。
7. 点击 "确定"。
9. 在左窗格中的 "*证书 (本地计算机)*"下，如果您导入的证书是自签名的，则点击 "可靠根证书机构"，然后点击 "证书"。如果不是自签名的，则点击 "个人"。
10. 在菜单栏上，点击 "操作 » 所有任务 » 导入..."，然后点击 "下一步"。
11. 输入要导入证书的文件路径 (必要时请使用浏览按钮)，然后点击 "下一步"。
12. 点击 "下一步"，然后点击 "完成"。

使用 Let's Encrypt 来管理您的证书

Let's Encrypt 是一个证书颁发机构，通过专门设计的自动化流程来为 "传输安全层 (TLS)"加密提供免费的证书，该流程使您可以免于现在复杂的手动创建、验证、签名、安装和续订用于保护网站安全的证书。点击 "配置 Let's Encrypt"，位于加密 102 页面，来打开 "Let's Encrypt PowerShell更新"页面，将帮助您轻松配置并运行 PowerShell脚本，它包含在 "SecurityGateway\LetsEncrypt"文件夹中。

Let's Encrypt PowerShell更新

要支持使用 Let's Encrypt 的自动化流程来管理证书，此屏幕来帮助您轻松简便地配置和运行 PowerShell脚本，位于 "SecurityGateway\LetsEncrypt"文件夹。使用此页面来配置和运行脚本，将使一切为 LetsEncrypt 准备就绪，包括将一些必要的文件放置在 SecurityGateway HTTP (模板)的目录中来完成 http-01 挑战。它使用 HTTP 服务器主机名称 107 作为证书的域 (如果此项为空，它将使用默认域 76)，检索证书、将其导入 Windows、并配置 SecurityGateway 来使用正在使用 SecurityGateway XMLRPC API 的证书。

注意：使用 Let's Encrypt 需要 PowerShell 5.1 或更高版本，以及 .NET Framework 4.7.2 或更高版本。此外，必须设置 SecurityGateway 的 HTTP 端口 107 设置来监听 80 端口，否

则 HTTP 质询将无法完成，脚本也将无法工作。

自动更新 LetsEncrypt证书
如果您希望通过 Let's Encrypt 脚本自动创建和更新 SSL/TLS 证书，请点击此框。将根据下方的 *"更新间的天数"*设置，证书将每隔 10~60 天更新一次。

当前密码
包含您的密码将为脚本创建一个 API 令牌来访问 SG XML API。不保存该密码。只是更新设置时这不是必要的。

主机名称 (用逗号分隔多个主机名称)
如果您希望在证书中设置备用主机名，请在此处指定这些主机名，并用逗号分隔。您无需在列表中包含 HTTP 服务器主机名 107。例如，如果您的主机名是 "mail.example.com"，而且您希望使用备选的 "imap.example.com"主机名，则您只需在此处包含 "imap.example.com"。如果您不想使用任何必选主机名，则将该选项留空。**请注意：**如果您包含主机名，则必须完成 Let's Encrypt 的 HTTP 质询，以验证您的服务器对该主机名的控制权。如果未完成全部质询，将无法继续处理。

用于通知的管理员邮件
如果您希望在 Let's Encrypt 更新期间发生错误时收到通知，请在此处指定管理员电子邮件地址。

使用 ECDSA 证书
如果您希望使用基于 ECDSA 的证书,而不是 RSA 证书，请选中此框。

使用预演服务器(staging server)
在您需要测试 Let's Encrypt 时使用此项。

更新间的天数 (10-60)
使用此选项可以指定从 10~60 天内更新证书的频率。默认设置是 60 天。

立即运行
点击这个按钮来立即运行脚本。

删除旧证书(过期 > 30 天前)
默认情况下，SecurityGateway 将删除过期时间大于 30 天的任何旧证书。如果您不希望自动删除这些证书，请不要勾选该复选框。

查看 LetsEncrypt脚本日志文件
点击此按钮来查看 Let's Encrypt 脚本的日志文件。

下次更新前的天数
此项显示在自动更新证书前还剩余多少天，按照在上方设置的*更新间的天数 (10-60)*。

命令行：
这将显示运行脚本时将使用的命令行文本。当您在此页面上进行更改时，文本会实时更新。

3.6.1.1 Let's Encrypt PowerShell 更新

Let's Encrypt 是一个证书颁发机构，通过专门设计的自动化流程来为"传输安全层（TLS）"加密提供免费的证书，该流程使您可以免于现在复杂的手动创建、验证、签名、安装和续订用于保护网站安全的证书。点击"配置 Let's Encrypt"，位于加密[102]页面，来打开"Let's Encrypt PowerShell 更新"页面，将帮助您轻松配置并运行 PowerShell 脚本，它包含在"SecurityGateway\LetsEncrypt"文件夹中。

Let's Encrypt PowerShell 更新

要支持使用 Let's Encrypt 的自动化流程来管理证书，此屏幕来帮助您轻松简便地配置和运行 PowerShell 脚本，位于"SecurityGateway\LetsEncrypt"文件夹。使用此页面来配置和运行脚本，将使一切为 LetsEncrypt 准备就绪，包括将一些必要的文件放置在 SecurityGateway HTTP（模板）的目录中来完成 http-01 挑战。它使用 HTTP 服务器主机名称[107]作为证书的域（如果此项为空，它将使用默认域[76]），检索证书、将其导入 Windows、并配置 SecurityGateway 来使用正在使用 SecurityGateway XMLRPC API 的证书。

注意：使用 Let's Encrypt 需要 PowerShell 5.1 或更高版本，以及 .NET Framework 4.7.2 或更高版本。此外，必须设置 SecurityGateway 的 HTTP 端口[107]设置来监听 80 端口，否则 HTTP 质询将无法完成，脚本也将无法工作。

自动更新 LetsEncrypt 证书
如果您希望通过 Let's Encrypt 脚本自动创建和更新 SSL/TLS 证书，请点击此框。将根据下方的*"更新间的天数"*设置，证书将每隔 10~60 天更新一次。

当前密码
包含您的密码将为脚本创建一个 API 令牌来访问 SG XML API。不保存该密码。只是更新设置时这不是必要的。

主机名称（用逗号分隔多个主机名称）
如果您希望在证书中设置备用主机名，请在此处指定这些主机名，并用逗号分隔。您无需在列表中包含 HTTP 服务器主机名[107]。例如，如果您的主机名是"mail.example.com"，而且您希望使用备选的"imap.example.com"主机名，则您只需在此处包含"imap.example.com"。如果您不想使用任何必选主机名，则将该选项留空。**请注意：**如果您包含主机名，则必须完成 Let's Encrypt 的 HTTP 质询，以验证您的服务器对该主机名的控制权。如果未完成全部质询，将无法继续处理。

用于通知的管理员邮件
如果您希望在 Let's Encrypt 更新期间发生错误时收到通知，请在此处指定管理员电子邮件地址。

使用 ECDSA 证书
如果您希望使用基于 ECDSA 的证书,而不是 RSA 证书，请选中此框。

使用预演服务器(staging server)
在您需要测试 Let's Encrypt 时使用此项。

更新间的天数（10-60）
使用此选项可以指定从 10~60 天内更新证书的频率。默认设置是 60 天。

立即运行
点击这个按钮来立即运行脚本。

删除旧证书(过期 > 30 天前)
默认情况下，SecurityGateway 将删除过期时间大于 30 天的任何旧证书。如果您不希望自动删除这些证书，请不要勾选该复选框。

查看 LetsEncrypt脚本日志文件
点击此按钮来查看 Let's Encrypt 脚本的日志文件。

下次更新前的天数
此项显示在自动更新证书前还剩余多少天，按照在上方设置的*更新间的天数 (10-60)*。

命令行：
这将显示运行脚本时将使用的命令行文本。当您在此页面上进行更改时，文本会实时更新。

3.6.2 HTTP 服务器

HTTP 服务器页面用来配置各种有关 SecurityGateway 网络页面的设置。您可指定在 SecurityGateway 创建的登录链接中使用的主机名，HTTP 和 HTTPS 端口，以及其他相关的 HTTP 设置。

服务器

主机名(用于创建登录链接)：
这是 SecurityGateway 在发送给用户和管理员的邮件中创建登录链接时将使用的主机名。例如，如果您的用户在连接 SecurityGateway 时需要使用的 URL 是 "https://sg.example.com:..."，请在这个框中输入 "sg.example.com"。SecurityGateway 将自动使用 "https://"，如果加载了 SSL 证书 100 或启用了下方的 *"将 HTTP 请求重定向到 HTTPS"*选项。否则它将使用 "http://"。此外，如果 SecurityGateway 设置为侦听非默认 https 或 http 端口，则相应的端口将自动添加到 URL 中。

HTTP 端口(逗号分隔)：
这是 SecurityGateway 的网络界面将使用的 HTTP 端口。当通过您用户的网络浏览器连接 SecurityGateway 的时候，他们需要在 URL 的冒号后输入这个端口号。例如，"http://sg.example.com:4000"。您可以输入多个端口，由逗号分隔。默认的端口是 4000。

HTTPS 端口(逗号分隔)：
这是用于 HTTPS 连接到网络界面时，SecurityGateway 将监控的 HTTPS 端口。连接到这个端口的用户需要在 URL 中使用 "https"并在冒号后输入端口号(比如，"https://sg.example.com:4443")。您可以输入多个端口，由逗号分隔。默认的端口是 4443。

绑定套接字到这些 IPs (逗号分隔)：
如果您希望限制 SecurityGateway 接收指向特定 IP 地址的连接，请在此处输入它们，由逗号分隔。

HTTP 请求的线程号
这是针对 HTTP 请求，SecurityGateway 将使用的线程号码。默认值为 5。

将 HTTP 请求重定向到 HTTPS
如果您希望将所有 HTTP 请求重定向到 HTTPS，请选中此框。如果您选择使用此选项，那么您必须确保您已为该域安装了一个有效的 SSL/TLS 证书 103。

为 HTTPS 请求添加 HSTS 报头
默认情况下，"HTTP 严格传输安全(HSTS)"报头被包含在 HTTPS 响应中。当支持 HSTS 的浏览器收到 HSTS 报头，并且 SSL 证书有效时，以后对同一域发出的 HTTP 请求将自动升级为 HTTPS。

存在时间最大值 [XX]秒
这是 "max-age="参数值，被包含在 HSTS 报头中。它是指示浏览器记住 HSTS 策略的时间。默认的设置是 63072000 秒或 2 年。

...包含子域
如果您希望报头包含 "includeSubDomains"指令，请勾选此框，这将指示浏览器将策略视为适用于网站的所有子域。

将域添加到 HSTS 预加载列表
如果您希望将 preload (预加载)指令添加到 HSTS 报头，请使用此项。

除非您确定要将域添加到所有主流浏览器的内置 "HSTS 预加载列表"中，否则您不应使用 "预加载"选项。当一个域被添加到 "HSTS 预加载列表"时，这意味着浏览器在连接到该域或其任何子域时，必须始终使用 HTTPS，如果您不打算这样做，这可能会阻止指向子域的合法连接。此外，一旦您的域被添加到 "HSTS 预加载列表"中，要将其从列表中删除可能既困难又耗时。

有关 "HSTS 预加载列表"的更多信息，请访问：
https://hstspreload.org/

配置

启用会话超时
启用该选项时，用户或者管理员如在以下指定的分钟内未进行任何操作将会自动登出网络界面。默认情况下启用此项。

在 [xx]分钟后注销用户
这是用户或管理员将自动登出网络页面前所允许的非活动状态持续的分钟数。该选项的默认设置是 15 分钟。

3.6.3 DNS 服务器

配置

使用 Windows DNS 服务器
选择此项时，SecurityGateway 将使用在您 Windows TCP/IP 配置中找到的所有 DNS 服务器。它会在每次查询操作中依次试验各个 DNS 服务器，直到找到完整的 DNS 服务器列表或首个能够有效工作的 DNS 服务器。

使用手动配置的 DNS 服务器
如果您希望指定 SecurityGateway 所使用的特定 DNS 服务器，请使用该选项。在执行 DNS 查询时它将按序使用在此处指定的所有 DNS 服务器。它会在每次查询操作中依次试验各个服务器，直到找到完整的 DNS 服务器列表或首个能够有效工作的 DNS 服务器。

3.6.4 IPv6

SecurityGateway 将自动检测您系统支持的 IPv6 能力级别和可用双栈；否则 SecurityGateway 将单独监控这两个网络。

配置

...仅接受 IPv4 连接
如果您希望仅接受 IPv4 连接请选择此项。

...仅接受 IPv6 连接
如果您希望仅接受 IPv6 连接请选择此项。

...接受 IPv4 或 IPv6 连接
如果您希望接受 IPv4 和 IPv6 连接，请选择此项。这是默认设置，而且 SecurityGateway 将在可能时比 IPv4 优先考虑 IPv6。

在可能时连接到出站 IPv6 主机
如果希望 SecurityGateway 尽可能连接到出站 IPv6 主机，请启用此选项。

3.6.5 目录

该页面列出了 SecurityGateway 所使用的文件夹，用来管理不同类型的文件。您可通过改变任何以下路径然后点击工具栏上的保存，来自定义文件夹的位置。

目录设置

附件：
该文件夹用来让 SecurityGateway 存储邮件中所包含的附件，只要这些是驻留在 SecurityGateway 服务器上的邮件。

此文件夹的内容不包含于 SecurityGateway 的内部备份[118]和还原[119]文件中。如果您希望备份附件，那么请使用第三方备份软件或者采取一些其他外部措施。

备份：
此处存储的是备份[118]文件。为了实现最优的性能，我们建议在不同的物理磁盘驱动器上设置此文件夹。

日志：
SecurityGateway 的日志文件存储在此处。

入站队列：
SecurityGateway 将把此文件夹用作入站邮件的邮件队列。

临时文件夹：
这是将用来处理的临时文件夹。

贝叶斯学习反垃圾邮件：
若使用了贝叶斯学习[129]功能，此文件夹中应该放置的是非垃圾邮件。

贝叶斯学习垃圾邮件：
若使用了贝叶斯学习[129]功能，此文件夹中应该放置的是垃圾邮件。

崩溃内存转储文件：
如果 securitygateway.exe 进程发生崩溃，这是自动生成内存转储文件的位置。

3.6.6 磁盘空间

磁盘空间页面用于配置 SecurityGateway 来监控您的可用磁盘空间。它包含的选项可用于向管理员发送警告邮件，并/或在磁盘空间不足时停止接收邮件。

启用磁盘空间检查引擎
启用此选项时，SecurityGateway 将监控目录[109]页面上所参考的所有卷上的可用磁盘空间。默认情况下启用此项。

若可用磁盘空间不足[xx]MB，则向全局管理员发送警告
启用了此选项后，当磁盘空间低于所指定的千字节值时，将向全局管理员[50]发送一封警告邮件，单位是(MB)。默认值为 1000 MB，且根据默认已启用该选项。

如果可用磁盘空间低于[xx]MB，则禁用 SMTP 引擎
有了这个选项后，若磁盘空间低于指定值，SecurityGateway 将禁用 SMTP 引擎，那么将不再接收任何邮件。默认值为 100 MB，且根据默认已启用该选项。

3.6.7 品牌管理/自定义图片

该页面所提供的选项，用于定制出现在登录页面和导航工具栏上的横幅图片。

自定义

使用默认图片
点击该选项来使用 SecurityGateway 的默认图片。

使用自定义图片
如果您希望指定 SecurityGateway 所使用的自定义图片，请选择该选项。

登录页面图片

这就是 SecurityGateway 即将显示在登录页面上的主图片。该部分包含默认的图片大小并为您提供选项来上传您的自定义图片。

导航工具栏图片

这张是您登录到 SecurityGateway 时显示在导航工具栏顶部的图片。该部分包含默认的图片大小并为您提供选项来上传您的自定义图片。

例外 - 域

当配置这些设置时，如果您在页面顶部的 *"针对域："* 下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。点击 *"查看/编辑"* 相应域的链接来查看或编辑其自定义设置，或点击 *"重置"*，将域设置重置为默认的全局值。

3.6.8 查看配置

当在导航菜单上点击 *"设置/用户»系统*下的*查看配置"*，该页将显示当前所有的 SecurityGateway 设置。当试图为 SecurityGateway 服务器诊断故障或寻求技术支持时，该功能会很有用。要将当前配置保存为 XML 文件，可在工具栏上点击 *"下载 XML 文件"*。然后在打开的对话框上点击 *"保存"*，选择文件保存位置，并再次点击 *"保存"*。

3.6.9 集群

SecurityGateway 的集群功能的设计旨在：在网络上的两个或多个 SecurityGateway 服务器之间共享您的配置。这使您可以使用负载均衡硬件或软件，在多个 SecurityGateway 服务器之间分配电子邮件负载，从而可以通过减少网络拥塞和过载，并最大化电子邮件资源来提高速度和效率。如果一台服务器发生硬件或软件故障，该功能还有助于确保电子邮件系统中的冗余。

在决定是否在网络上设置 SecurityGateway 集群时，需要考虑以下几点：

节点

一个 SecurityGateway 集群将具有一个主节点和一个次节点。一台 SecurityGateway 服务器将被指定为主服务器，而其他所有服务器将被指定为次服务器。

- 集群中的每个节点需要运行相同版本的 SecurityGateway。
- 集群中的每个节点都需要自己的 SecurityGateway 注册密钥。您不能在多个节点上使用相同的密钥。
- 集群上的每个节点应位于同一个网络。集群系统未被设计成具有在地理位置上分离的节点。

- 集群中的所有节点应设置为相同的时区，并设置为完全相同的时间。每个节点上系统时间的实质差异可能会导致问题。
- 可以从集群中的任何节点进行配置变更。当进行配置更改时，所有其他节点都将收到变更通知。注意：HELO 域名[76]是一个按服务器的设置，因此可以在集群中的每台服务器上设置为唯一值。
- 主节点负责维护任务，例如贝叶斯学习。

路由

SecurityGateway 不处理去往或来自特定节点的任何流量的路由。我们建议您使用第三方负载均衡器来处理流量路由。

负载均衡器中的粘滞 (Sticky)会话是必需的，以便来自同一 IP 的所有流量都路由到同一主机。对于那些登录 SecurityGateway 的 Web 界面的用户而言，粘性会话最为重要，因此，如果有人登录到特定的服务器，则该会话的所有流量都将被路由到同一服务器。

共享的数据库和文件夹位置

在 SecurityGateway 集群中，所有服务器共享相同的数据库和一组特定的文件夹。因此，所有节点必须位于同一网络上，并且所有共享位置都必须对所有节点都可访问。由于 SecurityGateway 服务默认情况下以 LocalSystem 账户运行，又因为 LocalSystem 无权访问任何网络资源，您必须配置该服务[115]来使用有权访问这些网络位置的账户。还请参阅："下方的配置 SecurityGateway 来使用可访问网络的数据文件夹[113]。

归档

要使用含有集群的归档[78]，您的 "归档"设置将需要配置为使用 Firebird 数据库服务器，并使用网络路径，以便所有节点都可以访问归档存储。

证书

- HTTPS 设置 (包括证书)是针对每个节点的，并且需要为添加到集群的任何节点指定 HTTPS 设置。证书存储在每个节点上，而不存储在数据库中。因此，如果您希望在每个节点上使用相同的证书，则需要在每个节点上手动导入该证书，并将每个 SecurityGateway 配置为使用该证书。
- STARTTLS 允许列表和要求 STARTTLS 列表[100]配置是共享的。
- SecurityGateway 的 LetsEncrypt 选项目前不支持次节点。

设置集群

升级您的数据库

如果您希望使用集群，并将 SecurityGateway 从早期版本更新为 7.0 或更高版本，则首先需要使用内含的 SGDBTool.exe 来将您的 SecurityGateway 数据库文件从 Firebird 2.x 转换成 Firebird 3.x。如果这是 SecurityGateway 7.0 的新安装或更高版本，则可跳过此步骤，因为您的版本已在使用 Firebird 3.x 数据库。

请按照以下步骤升级数据库：

1. 停止 SecurityGateway 服务 (点击 SecurityGateway 开始菜单文件夹中的 "**停止 SecurityGateway**"或使用 "服务"控制台)。

2. 打开 Windows 命令行提示。
3. 切换到您的 \SecurityGateway\app\ 文件夹。
4. 输入：**sgdbtool.exe -convertfb3** 并按回车。

这会将您的 Firebird 2.x 数据库文件作为 "SecurityGateway.fb2"另存为一份副本。然后它将使用 Firebird 3.x 运行时恢复您的数据库，并将其保存为 "SECURITYGATEWAY.FBD"。如果您正在使用 "归档[78]"，这也将升级任何归档数据库文件。

配置 SecurityGateway 来使用可访问网络的数据文件夹。

SecurityGateway 集群中的所有节点共享同一数据库和一组公用的多个文件夹。因此，所有节点必须位于同一网络上，并且您必须确保每个节点的 Windows 服务[115]被配置为使用有权访问共享位置的账户。您还必须确保正确配置每个节点来使用这些位置。如果需要将共享文件夹的内容移动到新位置，以便与所有节点共享它们，则必须手动移动它们。SecurityGateway 不会为您迁移现有文件。将使用以下共享的文件夹，并能从目录[109]页面和集群页面对其进行配置（贝叶斯复制除外，该贝叶斯复制只能从群集中配置）：

- **邮件数据**（例如 \\Share01\SecurityGateway\Messages\）
- **邮件日志/SMTP 记录**（例如 \\Share01\SecurityGateway\Transcripts\）
- **附件**（例如 \\Share01\SecurityGateway\Attachments\）
- **贝叶斯学习非垃圾邮件**（例如 \\Share01\SecurityGateway\BayesHam\）
- **贝叶斯学习垃圾邮件**（例如 \\Share01\SecurityGateway\BayesSpam\）
- **贝叶斯复制**（例如 \\Share01\SecurityGateway\BayesReplication）**注意：**该文件夹对于集群是唯一的。主节点将其贝叶斯数据库复制到该位置，其他节点从该位置复制该数据。

请注意：数据库位置和凭据在安装过程中指定，或通过使用现有安装的 SGDBTool.exe（请参阅："下方的配置 SecurityGateway 来使用外部数据库服务器[114]。

归档存储

如果您正在使用归档[78]功能，您也需要将您的 "归档存储库"重新定位到网络可访问的位置，并且每个归档数据库文件都需要移动到 Firebird 数据库服务器。还请参阅："使用含有集群的归档[114]。

设置 Firebird 3 数据库服务器

要使用集群，您必须将 Firebird 3 数据库服务器安装在集群中每个节点均可访问的网络位置。

要设置您的 Firebird 3 服务器：

1. 下载 Firebird 3 数据库服务器.
2. 在所有节点都可以访问的机器上运行安装程序。
3. 接受 "许可证协议"并点击 "下一步"。
4. 请阅读该信息并点击 "下一步"。
5. 选择一个文件夹并点击 "下一步"。

6. 在 "选择组件"上点击 "下一步"。
7. 为 "开始菜单"文件夹选择一个名称 (或点击 "不创建开始菜单文件夹")然后点击 "下一步"。
8. 将 "选择其他任务"选项设置为默认值 (例如 "超级服务器"模式，"作为服务运行"和 "复制客户端库")，并点击 "下一步"。
9. 输入并重新输入 SYSDBA 密码 (以后将需要 "SYSDBA"用户名和此密码)，并点击 "下一步"。
10. 点击 "安装"。
11. 点击 "下一步"。
12. 点击 "完成"。

配置 SecurityGateway 来使用外部数据库服务器。

在 SecurityGateway 集群中，必须将每个节点配置为连接到相同的数据库文件，该文件必须位于您在上一节中设置的 Firebird 3 数据库服务器上。要设置 SecurityGateway 使用外部的数据库服务器：

1. 在 Firebird 服务器上，为您的数据库文件创建一个文件夹 (例如 C:\Databases)。
2. 将您主要的 SecurityGateway 数据库文件 (例如 \SecurityGateway\App\SECURITYGATEWAY.FBD) 复制到该位置。
3. 在您的 SecurityGateway 服务器上，打开 Windows **命令行提示**。
4. 切换到您的 \SecurityGateway\app\ 文件夹。
5. 输入：**sgdbtool.exe -setdbconnect** 并按"回车"。
6. 对于 "使用内嵌的 Firebird 数据库 Y/N？"请输入 **N** 并按 "回车"
7. 对于 "输入 Firebird 服务器 IP"，输入 Firebird 服务器的 IP 地址 (例如 10.10.0.1)，然后按 "回车"。
8. 按 "回车"来应对 "输入 Firebird 服务器端口 (默认值为 3050)"。
9. 对于 "输入 Firebird 数据库路径或别名"，键入复制到 Firebird 服务器的数据库文件的完整路径。(例如C:\Databases\SECURITYGATEWAY.FBD)，并按 "回车"。
10. 按 "回车"来应对 "输入 Firebird 数据库用户名 (默认值为 SYSDBA)"。
11. 对于 "输入 Firebird 数据库密码 (默认的主密钥)"，键入在安装 Firebird 3 服务器时创建的密码，然后按 "回车"。

现在，您的 SecurityGateway 主节点应连接到外部数据库服务器。

使用含有集群的归档。

要使用含有集群的归档[78]：

1. 在 Firebird 服务器上为归档数据库文件创建一个或多个文件夹 (例如 "c:\databases\Archives\Example.com，""..\Archives\company.com")。
2. 为每个归档存储的存储位置[87]创建网络可访问的文件夹。
3. 将所有归档存储文件复制到这些新位置。

4. 编辑每个归档存储[87]存储位置来使用指向其新位置的 UNC 文件路径。
5. 将您的每个 "归档存储"编辑成 *"连接到 Firebird 数据库服务器实例"*，并为每个数据库文件输入 *"数据库路径/别名名称"*。
6. 按需编辑您的 "自动归档存储创建[82]"设置，设置 UNC 文件路径并修改宏使用来支持集群。

将节点添加到您的集群

要将新的 SecurityGateway 安装添加到您的集群：

1. 在要用作新节点的计算机上运行 SecurityGateway 安装程序。
2. 在安装过程中，选择 "连接到外部的数据库服务器"选项，然后使用您在上一节中输入的信息。
3. 正常进行其余的安装。
4. 请确保在 Windows 服务[115]部分使用正确的账户凭证，并且您已将新服务器配置为使用 UNC 文件路径连接到共享数据文件夹。
5. 将所有必要的 SSL 证书复制到新计算机上。

Active/Active 数据库复制

如果您希望对集群使用 active/active 数据库复制，SecurityGateway 确实支持该功能，但它需要外部复制工具，并且其配置超出了本帮助文件的范围。有关如何配置集群来使用 active/active 复制的要求和指南，请参阅 PDF 文档：SecurityGateway: Configuring Active-Active Database Replication。

3.6.10 Windows 服务

默认情况下，SecurityGateway Windows 服务在本地系统账户下运行。不过该账户没有访问网络驱动器的权限。因此如果您需要在不同的账户下运行服务，例如使用集群[111]这种情况下，则此页上的选择可以指定该账户及其凭证。

本地系统账户
默认情况下，SecurityGateway Windows 服务在本地系统账户下运行。

此账户
如果您需要在不同的账户下运行服务，请在此处输入该账户的*登录名*、*密码*和*域*。

3.7 数据库

*设置/用户*菜单的 "数据库"部分包含链接转至以下四个页面，处理 SecurityGateway 保存的数据类型和数量，以及备份和恢复 SecurityGateway 数据库：

配置[118]—使用此页面可指定数据库写入模式，即数据是以同步方式还是异步方式写入磁盘。

数据保留 116—使用此页面来配置 SecurityGateway 将保留邮件数据库记录，邮件内容以及每封邮件的 SMTP 会话脚本的时间。你也可以指定在何种情况下要保留或删除邮件内容。数据库维护的操作是每晚半夜时进行，此页面上的所有值都将保留数日。

备份 118—使用备份页面来调试您 SecurityGateway 数据库的自动备份。您可调试整个数据库的备份，或者仅调试配置与设置。您也可以指定要存储的旧备份文件的数量。

还原 119—还原页面列出了由目前保存在您系统里的备份页面而创建的所有配置和数据库备份文件。您可以自该页下载文件，删除文件，并自这些文件还原您的配置或整个数据库。

3.7.1 配置

使用此页面可指定数据库写入模式，即数据是以同步方式还是异步方式写入磁盘。

数据库写入模式

同步写入数据
当选择此选项时，数据立即刷新到磁盘。数据库写入处理直到数据被物理写入磁盘才会完成。这是默认选择，对您的数据最安全。

异步写入数据
当选择此选项时，操作系统控制何时将数据物理写入磁盘。182/5000 该选项提供了卓越的性能，但是如果服务器和/或数据库发生停电或其他不受控制的关闭时，则会增加数据库损坏的风险。只有当同步写入模式的性能不足时才推荐使用异步写入模式。系统受到可靠的不间断电源 (UPS)保护并保持数据库备份至关重要。

3.7.2 数据保留

使用此页面来配置 SecurityGateway 将保留邮件数据库记录，邮件内容以及每封邮件的 SMTP 会话脚本的时间。你也可以指定在何种情况下要保留或删除邮件内容。数据库维护的操作是每晚半夜时进行，此页面上的所有值都将保留数日。

邮件数据库记录

在下面指定希望保留邮件数据库记录的时间。报表将限制在此期限内。期限越长，数据库越大。

不执行任何操作
若您不希望删除邮件数据库记录，请选择此选项。

在 [xx]天后删除记录
如果您希望每晚半夜时删除旧的数据库记录，请选择此选项并指定您希望每个记录所保留的天数。这是一个默认的选项，且记录保存期限为 30 天。

邮件内容

根据默认，当一份邮件不再需要时，其内容将被删除，例如，邮件已成功发送至收件人，邮件从隔离中删除，等等。不过，保存每份邮件的内容对于调试有所帮助，下方提供的选项用来防止在许多不同的情况下邮件被自动删除。根据默认，这些选项都已禁用。

启用这些选项可能会造成性能降低，还能拥有一个更大的数据库。

邮件成功发送后不要删除邮件内容
即使邮件已成功发送至收件人服务器，您若还是希望保留邮件内容，请点击此选项。

当一封邮件从隔离中删除时，不要删除邮件内容
邮件从隔离中删除后，您若不希望删除一封已隔离的邮件内容，请启用此选项。

当一封邮件被拒绝时，不要删除邮件内容
若启用了此选项，那么即使在接受邮件后将其拒收，SecurityGateway 也不会删除邮件内容。

在永久性投递失败后不要删除邮件内容
若您希望保留碰到永久性投递失败情况的邮件，例如收件人无效的情况，请选择此选项。

不要删除未完成邮件的邮件内容
若您不希望删除未完成邮件的内容，请启用此选项。

邮件脚本

为每封邮件保留 SMTP 会话和 SIEVE 规则引擎的详尽日志。这些邮件记录对于故障诊断和调试很有帮助，然而它们确实造成了数据库规模的增长。

处理 (以上)邮件数据库记录
这是默认选项。选中后，将根据下方邮件数据库记录区段里已选中的选项来处理邮件脚本。将旧的邮件数据库记录删除后，会话脚本同时也被删除。

在 [xx]天后删除邮件脚本
若您希望将邮件脚本保留一个具体的天数，那么点击此选项并指定您想保留的天数。

不要存储邮件脚本
若您不希望存储邮件脚本，请使用此选项。

带宽信息

在 [xx]天后删除带宽信息
若您希望在每晚半夜时删除旧的带宽使用信息，请启用此选项并指定天数。

3.7.3 备份

使用备份页面来调试您 SecurityGateway 数据库的自动备份。您可调试整个数据库的备份，或者仅调试配置与设置。您也可以指定要存储的旧备份文件的数量。备份文件列于还原 119 页面。

要实现最优的性能，我们推荐在不同的物理磁盘驱动器上查找备份文件夹（在 目录 109 页面上所指定的）。另外，在 SecurityGateway 服务仍在运行的情况下，我们不推荐使用第三方备份软件或者其他外部备份程序来备份 SecurityGateway 的数据库文件。在服务仍在运行的同时，该页面上的内部选项可以用来定期备份数据库。如果您想要使用某些外部备份程序，你应该先暂停服务，或者使用外部程序仅仅用来备份由 SecurityGateway 内部创建的备份文件。最后，SecurityGateway 的内部备份选项不备份附件 109 文件夹里的内容。如果您希望备份附件，那么请使用第三方备份软件或者采取一些其他外部措施。

自动备份

不执行自动备份
这是默认选项。如果选择了该选项，SecurityGateway 将不会自动备份数据库或者服务器配置。

每隔 [xx] 天在 [xx:xx] 时自动备份配置数据。
如果您希望导出/备份 SecurityGateway 的配置，请选择该选项，但不是备份所有的数据库。指定从等待自动导出到真正实行导出之间相隔的天数。这些文件列于恢复 119 页面并且文件名以 “导出”开头。

当使用备份这种方法时，仅备份 SecurityGateway 的配置与设置，包括用户和域的信息，而不是备份整个数据库。结果是，如果您以此类型的备份文件来还原系统，那么您将丢失所有的邮件、会话脚本、报告和邮件日志等等——只还原配置和设置。

每隔 [xx] 天在 [xx:xx] 时自动备份整个数据库。
若您希望备份 SecurityGateway 的整个数据库，请选择该选项，其中包括了您的配置及设置、邮件日志 254、报告 266、脚本等等。指定从等待自动备份到真正实行备份之间相隔的天数。这些文件列于恢复 119 页面并且文件名以 “备份”开头。

附件 109 文件夹里的内容不包含于备份文件中。若您希望备份附件，那么请使用第三方备份软件或者采取一些其他外部措施。此外，在备份整个数据库时，尽管已包含了邮件日志 260，但是不包含日志文件 261。如果您希望备份日志文件，那么请使用第三方备份软件或者采取一些其他外部措施。

备份文件只保存 [xx]天。最旧的备份文件将被删除。
如果您只希望保存一个数量的备份文件并指定要保存的文件数，请点击此选择框。如果达到了最大的文件数，则每当创建了新的备份文件时将删除最旧的文件。默认情况下，禁用该选项。

手动备份

点击此处，现在就备份/导出配置数据
点击此链接，手动导出 SecurityGateway 的配置。此备份方法在功能上等同于上述的 *"自动备份配置数据..."* 选项。仅仅是以手动开始而不是自动开始，并且作为任何调度的自动备份的补充。

点击此处，现在就备份整个数据库
点击此链接，手动地备份 SecurityGateway 的整个数据库。此备份方法在功能上等同于上述的 *"自动备份整个数据库..."* 选项。仅仅是以手动开始而不是自动开始，并且作为任何调度的自动备份的补充。

3.7.4 还原


还原页面列出了所有的配置与数据库备份文件，该文件使用当前保存在您系统上的备份 118 页面创建。您可以自该页下载文件和删除文件，并自这些文件还原您的配置或整个数据库。

上传备份文件

使用浏览与上传选项以上传一个先前下载过的备份文件并将其添加至以下的还原列表。您可以在这之后使用该文件以还原您的配置或整个数据库，这取决于备份文件的类型。

浏览
点击该按钮以浏览您希望上传至以下还原列表的数据库或配置文件 文件应该预先从该页下载，并使用备份 118 页面上的选项创建。

上传备份文件
使用浏览按钮找到文件后，请点击该选项以将其上传至以上的还原列表。

还原

该列表包含的所有文件，都是自备份 118 页面创建，或使用以上的上传备份文件选项上传的。每个条目都包含文件名，该备份文件创建的日期与时间、文件大小、以及下载、删除或还原文件的链接。文件名以 "导出"开头的文件仅包含了配置日期。文件名以 "备份"开头的是整个数据库的备份文件。


要了解每种备份文件类型的更多详情，请参阅备份 118 页面。

下载
点击备份文件条目中的下载链接以下载该文件。可以使用以上的上传备份文件选项在稍后将文件再次上传至还原列表。下载文件不会将该文件从列表中删除。

删除
使用该链接以下载备份文件。如果您希望将文件从 SecurityGateway 移走但将其保存在其他的位置，在删除该文件前使用以上的下载选项。

还原
点击该链接以自 SecurityGateway 对应的文件还原其配置或整个数据库。在还原完成前，自备份文件创建起所作的所有更改都有可能丢失，SecurityGateway 也将不可用。还原完成后您还必须重新登录。执行前还将询问您是否确定这项操作。

3.7.5 高级

如果技术支持指示这样做，请使用此页面对数据库执行 SQL 语句。建议您在继续操作前执行数据库备份 118。

执行 SQL 语句

SQL 语句：
如果技术支持指示这样做，请在此框中输入 SQL 语句并点击 "执行"。将在下方更新框中显示检查 "结果"。

3.8 软件更新

使用此页面来检查是否存在可用的 SecurityGateway更新版本。您可以手动地检查更新或使用一个选项，让 SecurityGateway 自动检查更新。在找到一个更新时，您可以通过网络界面下载并进行安装。

配置

定期检查软件更新
若希望 SecurityGateway 于每晚午夜自动检查软件更新，请勾选此框。

点击此处立即检查软件更新
点击该链接自动检查软件更新。将在下方更新框中显示检查结果。

更新

此框中包含软件更新检查结果。存在可用的软件更新时将通知所有全局管理员 50，并提供一个链接，您可以使用该链接来打开软件更新详细信息页面，可用来下载和安装此更新。

软件更新详细信息

当更新检查显示出现软件更新，就会在仪表盘[9]和 "软件更新"页面的 "更新"部分上提供一个转至 "软件更新详细信息"页面的链接。该页面显示的是目前安装的软件版本，可以使用的版本，以及新版本的文件大小。还提供一个链接，以查看更新中的更改列表；还有一个指向下载和安装该更新的链接。

3.9 注册

该页面列出了您的产品注册信息，包括注册该产品的人名或公司、注册码、您的注册状态，例如许可证大小与其他相关信息。

SecurityGateway

该部分相关 SecurityGateway 产品的注册信息。

许可证名称：
在该名称下注册许可证

公司或分销商：
这是许可证上的您的公司或分销商。

SecurityGateway 注册码：
这是用于您注册码的选项框。输入您的注册码之后，请点击 *"保存"*。

注册状态
该选项框列出了您的注册状态，包括许可证大小和其他信息。

配置
当 SecurityGateway 向 MDaemon Technologies 请求更新的许可证文件时，可能会报告其运行的操作系统的版本。这些信息对我们确定支持哪些操作系统是很有帮助的。如果您不希望报告这些信息，请禁用此选项。

章节

4

4 安全

安全菜单有八个部分，具有各种工具以帮助您保护您的域与用户免受垃圾邮件、病毒、邮件滥用以及其他安全风险的侵扰。以下是对各个安全部分的简单概述。要了解更多详情，请参见各个部分。

反垃圾邮件 125
反垃圾邮件部分位于安全菜单之下，包含一些选项帮助您防范垃圾邮件或主动发送的垃圾邮件。在这部分下方列出了九个反垃圾邮件功能，包括通过使用启发式、贝叶斯分析、DNS、URI 阻止列表和灰名单等来识别和防止垃圾邮件的选项。

反病毒 146
反病毒部分位于安全菜单之下，包含一些选项以帮助您识别受病毒感染的邮件并防范它们侵扰您的用户。

反欺诈 148
"反欺诈"部分具有一些工具，可以帮助您识别来自伪造的或者"诈骗性"地址的邮件。该部分下有六个反诈骗功能，比如 DKIM 验证、发件人 ID、回呼验证等。

反滥用 172
"反滥用"部分包含一些工具，可以帮助您防范其他人滥用或者不恰当地使用您的邮件系统来中继垃圾邮件，防止其他人使用大量的带宽，或过于频繁地连接您的服务器等等。反滥用部分下有六个工具。

过滤
过滤部分包含两个功能：邮件内容过滤 195 与附件过滤 203。"邮件内容过滤"页面可以用来创建过滤规则以执行一系列操作。您可以创建规则以拒收满足某种条件的邮件，复制邮件或将邮件重新指向不同的地址，隔离邮件等等。附件过滤页面上的选项可以用于指定当邮件具有某一特定类型的附件时，将阻止或隔离该邮件。您可以全局性地或为每个域定义过滤限制。

阻止列表 205
阻止列表是一些列表，如果您希望阻止或者隔离某些邮件，会于此列出其邮件地址，主机与 IP 地址。默认情况下，那些邮件将在 SMTP 会话中被拒收，但是在"阻止列表操作"页面，您可以更改这项设置以隔离邮件。可以全局也可以为特定的域设置将采取的措施，并且阻止列表本身也可进行全局或特定域的设置。

允许列表 212
允许列表是邮件地址、主机和 IP 地址的列表，其邮件将不受多种安全限制的约束。启发式与贝叶斯、DNSBL、DKIM 验证以及 SecurityGateway 中几乎每一个其他的安全功能，都具有选项用于在发件人，主机，邮件等显示在适当的允许列表上时，将它们从中排除。每个允许列表都可以进行全局或特定域的设置。

Sieve 脚本 219
SecurityGateway 使用 Sieve 邮件过滤语言以执行许多功能，并且 Sieve 脚本页面会让您看见那些功能是是按什么顺序执行的。它还为您提供了 Sieve 脚本编辑器以让您可以用之创建您自己定制的脚本。

4.1 反垃圾邮件

安全[124]菜单下的反垃圾邮件部分中包含了帮助您放置垃圾邮件或者多余邮件的选项。这一部分下有九个反垃圾邮件功能：

爆发保护[126] - 爆发保护 (OP) 是一种革命性的实时反垃圾邮件与反病毒的技术，能够在垃圾邮件或病毒爆发的几分钟内前瞻性地自动保护您邮件的基本结构。由于爆发保护是专门为处理爆发情况而设计，所以它无法取代 SecurityGateway 中所包含的另一个更传统的反病毒及反垃圾邮件工具。除了其他工具以外，它还提供一层特殊的保护。

启发式与贝叶斯[129] — SecurityGateway 使用了一款高性能且流行的开源式自定义版本 SpamAssassin™ 项目，用于启发式规则与贝叶斯分类。启发式部件可通过一系列已知的垃圾邮件的常见特征来测试邮件，从而识别邮件是否是垃圾邮件。贝叶斯部件辨别垃圾邮件的方式是：首先解析邮件，然后将其与邮件令牌数据库相比较，该数据库是由您所提供的垃圾邮件及非垃圾邮件编译而成的。

DNS 阻止列表 (DNSBL)[134]该安全性功能允许您指定若干个 DNS 阻止列表服务（它们维持了中继垃圾邮件所知的服务器列表），每次有人试图发送邮件至您的其中一个域，都将对该邮件进行安全性检查。若连接的 IP 已被这些服务中的任何一项列入阻止列表，那么该邮件将被拒绝，隔离，或者标记。

URI阻止列表 (URIBL)[137] - URI 阻止列表是实时的阻止列表，基于在邮件正文中找到的统一资源标志符 (uniform resource identifiers)来阻止垃圾邮件或在垃圾邮件上添加标签。也称为垃圾邮件 URI 实时阻止列表 (SURBL)，URIBL 与 DNS 阻止列表的不同之处在于：它们不是用于根据报头的内容或连接的 IP 地址识别垃圾邮件。而是基于邮件的内容来阻止垃圾邮件。

灰名单[140]—灰名单是一项对抗垃圾邮件的技术，它通过告知发送方的邮件服务器 — 出现了一个暂时性的错误，必须稍后重新发送。因为当一封邮件无法发送时，垃圾邮件发送者们一般不再试图发送，不过合法的邮件服务器会这样做。灰名单帮助用户减少了所收到的垃圾邮件的数量。

反向散射保护[142] - "反向散射"指的是用户收到对其从未发送过的邮件的响应邮件。当病毒发送的垃圾邮件或邮件中包含伪造的"返回路径"地址时会发生反向散射。因此当其中一封邮件被收件人服务器拒收时，或如果收件人使用与其帐户相关的自动应答程序，响应邮件随之将指向您用户的伪造地址。为了对抗反向散射，SecurityGateway 使用私钥散列法来生成和插入特殊的时间敏感代码至用户出站邮件的"返回路径"地址。然后，当其中一封邮件遇到投递问题被弹回，或收到带有mailer-daemon@..."或者 NULL 反向路径的自动回复时，MDaemon 将检测到特殊代码并知道这是由您的联系人所发邮件的真实自动回复。若邮件不包含特殊代码或者代码已过期，将会被记录下来并且可拒收。

邮件总值[143]—SecurityGateway 是基于处理邮件过程中邮件所执行的测试数来为每封邮件计算一个邮件总值。实际上就是"垃圾邮件的总值"。邮件总值是用来判定一封邮件为垃圾邮件的可能性。邮件总值页面上的选项用来指定当邮件总值超出特定的阈值时所要采取的行动。在 SMTP 会话过程中，您可以为标记过的邮件设置阈值，将其作为垃圾邮件隔离或者拒收它们。

数据查询服务 (DQS)[145]数据查询服务 (DQS) 是一套 DNSBLs[134]，它们实时进行更新并由 Spamhaus Technology 运营，以便阻止超过 99% 的由电子邮件带来的威胁。DQS 需要由 Spamhaus Technology 提供的有效订阅和使用密钥。

Abusix[145] - Abusix Mail Intelligence™ 是一套实时的 DNSBLs[134]，其设计旨在阻止随邮件携带的威胁。Abusix Mail Intelligence 需要 Abusix 提供的有效订阅和使用密钥。

4.1.1 爆发保护

爆发保护(OP)是一种革命性的实时反垃圾邮件与反病毒的技术，能够在垃圾邮件或病毒爆发的几分钟内前瞻性地自动保护您邮件的基本结构。爆发保护是完全的内容不可知保护，这意味着它不依赖于严格的邮件内容词汇分析。因此不需要任何启发式规则、内容过滤或签名更新。此外，这表示它不会被附加的种子文件、"聪明"的拼写更改、社会工程策略、语言障碍或不同的编码技术所欺骗。相反地，OP 依据对于邮件结构和通过 SMTP 邮件分发特征的数学分析——分析与邮件传输相关联的"模式"，并从全世界收集的具有类似模式的数千万邮件中抽样与之进行比较，抽样和比较都是实时进行的。

由于全世界的邮件都在进行实时分析，因此能够在新一轮爆发的几分钟（通常是几秒钟）内提供保护。对于病毒来说，这种级别上的保护非常重要，因为病毒爆发后，传统的防病毒开发者通常需要数小时才能验证并提交病毒签名更新，这样将更新用于产品使用所需的时间则更长。在此期间，不带爆发保护的服务器容易遭受这种特定爆发的攻击。同样，对于垃圾邮件，在其没有被传统的基于启发式和内容的系统识别出来之前，爆发保护将经常花大量时间和精力分析这些垃圾邮件并创建安全的过滤规则。

不过值得注意的是，"爆发保护"功能不是传统反病毒和反垃圾邮件技术的替代品。而爆发保护实际上是为 SecurityGateway 中现有的基于启发式、签名和内容的工具顶层提供了另一层专门的保护。爆发保护专门用于处理大范围的爆发，而不是处理那些通过传统工具可以更为轻松捕获的旧的、特殊的或特定目标的邮件。

"爆发保护"基于 循环模式检测和零时技术。它的工作方式为：从您接收的邮件中提取模式，并与每天从全球无数来源采集的数百万封互联网邮件模式进行比较。它绝不会传播任何邮件的实际内容，也不会从提取的模式中获得任何邮件内容。

反垃圾邮件

启用反垃圾邮件爆发保护
默认启用爆发保护中的反垃圾邮件选项 将对接收的邮件进行分析，以查看其是否为进行中的垃圾邮件爆发的一种。这部分中其他的选项用于确定对作为一种爆发的邮件采取的措施，并用来指定免于进行 OP 处理的发件人。

如果爆发保护确定一封邮件为垃圾邮件：
以下选中的选项，在 OP 将一封邮件识别为垃圾邮件时，决定了对其采取的措施。

...拒收邮件
如果您希望在 OP 确定邮件为垃圾邮件爆发的一种时，在 SMTP 处理中阻止邮件，请选中该选项。这些邮件将不会被隔离或标记为垃圾邮件，也不会被投递至其目标收件人——服务器将拒绝这些邮件。

...隔离邮件
当选中该选项，在爆发保护将邮件识别为垃圾邮件时，会隔离它们。

...接受邮件
默认情况下，OP 将接收会被确认为垃圾邮件的邮件，并根据以下的 *"..添加 [XX] 点数至邮件总值"*选项调整其邮件总值。

...用 [文本]标记主题
默认情况下，该选项处于禁用状态。如果您启用该选项，那么在爆发保护确认邮件为垃圾邮件的时候，就会在邮件主题报头的开头添加文本。默认的添加文本是："*** 垃圾邮件 ***"，但是您可以根据自己的需求编辑该文本。

SecurityGateway 内部还有许多其他区域可以让您选择性地向主题报头添加文本，包括以下的另外两个爆发保护选项。当那些选项中的指定文本是一样的，仅会将该文本添加至邮件主题一次，即使那封邮件在各个选项下满足了条件。但是，如果您在一个或多个选项中更改了文本，那么还是会添加该自定义文本。比如，如果您在多个选项下，将文本全部设置为"垃圾邮件"，那么仅会将该文本添加至主题一次，不管它是否在多个选项下都满足了条件。但是如果您更改了其中一个选项下的文本，比如将文本改为"垃圾邮件*"，那么会添加两个标签。

...向邮件总值添加 [XX]点数
当爆发保护将邮件识别为垃圾邮件，使用该选项向邮件总值添加指定的点数。默认启用该选项，并向邮件总值添加 5.5 个点数。

即使 SecurityGateway 配置为接受邮件而不是拒绝或隔离邮件，但若邮件最终得分足够高，该邮件仍可能被拒绝或隔离，这取决于其他安全 124 选项和邮件评分 143 页上选项的配置。

如果爆发保护确定一封邮件为潜在的垃圾邮件：
当爆发保护无法进一步确定邮件是否为垃圾邮件时，会将这些邮件分类为"潜在的"垃圾邮件。以下选中的选项决定了 OP 将对那些邮件采取的措施。

...拒收邮件
如果您希望在 OP 确定邮件为潜在的垃圾邮件时，在 SMTP 处理中阻止邮件，请选中该选项。因为这些邮件仅被分类为*潜在的*垃圾邮件，所以不推荐使用这个选项，因为该选项会完全地拒绝邮件，而不是隔离或者为它们添加标签。

...隔离邮件
当选中该选项，爆发保护会隔离那些被分类为潜在的垃圾邮件的邮件。

...接受邮件
默认情况下，OP 会接收那些会被确定为潜在的垃圾邮件的邮件。如果选中该选项，你可以配置 OP 在之后根据以下的 *"..添加 [XX] 点数至邮件总值"*选项调整邮件的邮件总值。

...用 [文本]标记主题
默认情况下，该选项处于禁用状态。如果您启用该选项，那么在爆发保护确认邮件为潜在的垃圾邮件的时候，就会在邮件主题报头的开头添加文本。默认的添加文本是："*** 潜在的垃圾邮件 ***"，但是您可以根据自己的需求编辑该文本。

...向邮件总值添加 [XX] 点数
当爆发保护将邮件识别为潜在的垃圾邮件时，使用该选项向邮件总值添加指定的点数。默认启用该选项，并向邮件总值[143]添加 2.0 个点数。

如果爆发保护确定一封邮件为批发邮件：
有时 Outbreak Protection 不会将某些大规模分发的邮件识别为垃圾邮件，因为它们并不是发自已知的垃圾邮件发送者与僵尸网络 (bot-net)——在某些情况下，这些都是合法的批发邮件与时事通讯。OP 会将这些类型的邮件分类为批发邮件而不是垃圾邮件。以下的选项控制了将对这些邮件采取的措施。

...拒收邮件
该选项在 OP 将邮件分类为 "批发"时，会让 SecurityGateway 在 SMTP 会话期间拒绝邮件。不推荐使用该选项，因为它会导致一些广泛分发的合法邮件被拒绝。

...隔离邮件
如果您希望在爆发保护将邮件分类为 "批发"时隔离邮件，请选中该选项。

...接受邮件
默认情况下，OP 不会阻止或隔离批发邮件，因为被分类为 "批发"的邮件，可能只是某些大型的邮件发送列表的一部分或者其他一些类似的广泛分发的内容。

...用 [文本] 标记主题
默认情况下，该选项处于禁用状态。如果您启用该选项，那么在爆发保护确认邮件为批发邮件的时候，就会在邮件主题报头的开头添加文本。默认的添加文本是："*** 批发 ***"，但是您可以根据自己的需求编辑该文本。

...向邮件总值添加 [XX] 点数
当启用该选项，在 OP 将邮件分类为 "批发"时，会添加邮件总值。默认启用该选项并添加 3.0 个点数。

排除来自被列入允许列表的发件人的邮件
默认情况下，任何来自列于允许列表发件人[212]的邮件都从爆发保护的反垃圾邮件选项中排除。

排除来自经身份验证会话的邮件
默认启用该选项并用于将正在使用已验证会话的邮件从爆发保护中排除。

排除来自域邮件服务器的邮件
默认情况下，发送自您域邮件服务器[66]的邮件将从爆发保护中免除。如果您不希望将这些邮件从爆发保护限制中排除，请清除该复选框。

反病毒

启用反病毒爆发保护
默认启用爆发保护中的反病毒选项。将对接收的邮件进行分析，以查看其是否为进行中的病毒爆发的一种。这部分中其他的选项用于确定对作为一种爆发的邮件采取的措施，并用来指定免于进行反病毒爆发保护的发件人。

如果爆发保护确定一封邮件为受感染邮件：
以下选中的选项，在 OP 将一封邮件识别为受感染邮件时，决定了对其采取的措施。

...拒收邮件
默认情况下，当爆发保护确定邮件为病毒爆发的一种时，SecurityGateway 就会在 SMTP 会话期间拒绝这封邮件。

...隔离邮件
如果您希望在爆发保护将邮件确定为受感染时隔离邮件，请选中该选项。

排除发自被列入允许列表的 IP 地址和主机的邮件
如果您希望当邮件来自列于允许列表的 IP 地址[217]或列于允许列表的主机[215]时，将它从反病毒爆发保护中免除，请点击该复选框。

排除域邮件服务器
启用该选项时，发自您域邮件服务器[66]的邮件会从反病毒爆发保护中免除。

配置

使用 HTTPS 进行 "爆发保护"查询
默认情况下，"爆发保护"在连接到 "爆发保护"服务时使用 HTTPS 连接。

代理服务器设置

SecurityGateway 的爆发保护通过 HTTP 一定能与爆发保护的在线服务通信。如有必要您可以使用这部分的该选项为爆发保护指定将要使用的 HTTP 代理服务器。

例外 - 域

当配置这些设置时，如果您在页面顶部的 *"针对域："* 下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。在相应的域中点击 *"查看/编辑"* 链接来查看或者编辑其爆发保护设置，或点击 *"重置"* 来将域的设置重置回默认的全局值。

4.1.2 启发式和贝叶斯

SecurityGateway 针对启发式规则和贝叶斯分类，使用了一种高性能，可定制版本的 SpamAssassin™ 流行开源方案。通过这个程序的邮件会被指定一个依据其内容加以评判的分值。此外，要是您不希望使用内置的守护程序，SecurityGateway 还允许您使用您自己外部的 SpamAssassin™ 守护程序。

配置

使用启发式规则与贝叶斯分类来分析邮件。
默认情况下启用该选项，意味着邮件将通过启发式规则与叶贝斯分类系统，并被指定一个依据结果加以评判的 SpamAssassin 总值。如果您希望禁用这个系统并使此页的其他选项都不可用，请清除该复选框。

您可以将选项配置为自动更新您的启发式规则，这些管理叶贝斯分类的选项位于 SGSpamD Configuration[131] 屏幕上。您可以通过 *"点击此处来配置 SGSpamD"*[131] 这个链接到达该屏幕，这条链接位于以下 *"使用内置的本地 Spam Assassin 引擎 (SGSpamD)"* 的选项之下。

添加由 Spam Assassin 返回的总值到邮件总值
默认情况下，该选项是用来向邮件总值添加 Spam Assassin 总值的。在使用邮件评值选项时，向最终邮件总值添加 Spam Assassin 总值会为您带来更深层的反垃圾邮件保护并增加了捕获垃圾邮件的可能性，它将捕获那些因为分值不够高而不足以被 Spam Assassin 单独捕获或者其他个别的反垃圾邮件评值选项截获的垃圾邮件。

如果 Spam Assassin 总值大于或等于...拒收邮件
使用该选项为 Spam Assassin 总值指定一个拒收阈值。换言之，当邮件的 Spam Assassin 总值大于或等于该值时，它在处于 SMTP 会话中的那点时就被拒收了，而不是被隔离或者继续经由剩下的反垃圾邮件与邮件评值选项处理。因此，如果您将该选项与以下的"*如果 Spam Assassin 总值大于或等于……隔离邮件*"选项结合在一起使用时，拒收阈值应该要比隔离阈值设置的大。否则，邮件会因为其 Spam Assassin 总值而不再被隔离。任何总值高到足以被隔离的邮件在这之前就已经被拒收了。拒收阈值的默认值是 "12.0"。

如果 Spam Assassin 总值大于或等于……隔离邮件
如果您希望为 Spam Assassin 总值指定一个隔离阈值，请启用该选项。任何总值大于等于该值的邮件将被隔离。通过登陆 SecurityGateway，收件人与管理员可以查看与管理被隔离的邮件。如果你将该选项与以上 *"如果 Spam Assassin...拒收邮件"* 选项结合在一起使用，*"隔离邮件..."*选项的值要比 *"拒收邮件..."*选项的值设的低。该选项的默认值是 "5.0"。

您应该监控启发式与贝叶斯系统的执行，并在一段时间之后根据您的需要改进拒收与隔离阈值的设置。通常情况下，默认值将捕获大多数垃圾邮件，但相对的也会有极其少的漏报 (溜进来的未被识别的垃圾邮件)与误报 (被标志为垃圾邮件的非垃圾邮件)现象。默认拒收阈值 12 是一个良好的起点，因为在大多数情况下合法邮件的总值不会那么高。

例外

排除大于 [xx]KB 的邮件
如果您希望将较大的邮件从由启发式与贝叶斯系统扫描的邮件当中排除，在此指定一个需要的值 (以千字节的形式)。大型邮件不太会被视为垃圾邮件，将它们从扫描中排除可以节省大量的资源。

排除来自被列入允许列表的发件人的邮件
默认情况下，如果邮件源自允许列表 212 的发件人，该在默认情况下，SecurityGateway 将为该邮件豁免启发式和贝叶斯处理。如果您不希望排除这些邮件，请清除该复选框。

排除来自经身份验证会话的邮件
当 SMTP 会话来源已经验证，该选项用来将邮件从启发式与贝叶斯系统中排除。默认情况下启用此项。

排除来自域邮件服务器的邮件
默认情况下，来自您域邮件服务器 66 的邮件将从启发式与贝叶斯处理过程中排除。如果您不希望免除来自那些服务器的邮件，请不要勾选这个选项。

位置 (所有域)

使用内置本地 SpamAssassin 引擎 (SGSpamD)
如果您希望使用 SecurityGateway 的内置 SpamAssassin 引擎，它是作为一个单独的域——SecurityGateway Spam Daemon (SGSpamD)运行的，请选择该选项。要配置 SGSpamD，请点击 *"点击此处以配置 SGSpamD"*131链接。如果您希望使用一个运行在远程位置上的不同的 SpamAssassin 引擎，请选择以下的 *"使用远程 Spam Assassin..."*选项。

使用远程 SpamAssassin 守护程序 (SpamD)
如果您希望使用位于远程位置上的 SpamAssassin 守护程序而不是内置 SGSpamD 来扫描邮件，请选择该选项。

主机地址：
在此处指定远程 SpamD 的 IP 地址。

端口：
使用该选项来指定您远程 SpamD 运行的端口。

测试
点击该按钮来测试远程 SpamD 的连接。

例外 - 域

当配置这些设置时，如果您在页面顶部的 *"针对域："*下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。在相应的域中点击 *"查看/编辑"*链接以查看或者编辑其启发式与贝叶斯设置，或点击 *"重置"*来将域的设置重置回默认的全局值。

4.1.2.1 SGSpamD 配置

启发式规则系统将每封邮件的内容与一组静态规则进行比较，以确定邮件是否为垃圾邮件的可能性。每条规则有一特定分值，因而可根据邮件匹配的每条规则分值调整每封邮件的 SpamAssassin 分数。规则和分值会定期进行调整和更改，以跟上垃圾邮件的发展趋势。SecurityGateway 的 SGSpamD 可配置为以指定的时间间隔自动检查启发式规则的更新，或者您也可手动检查更新。

贝叶斯分类是一种可选的统计过程，用于对垃圾邮件和非垃圾邮件进行分析，以便随着时间的推移不断提高垃圾邮件识别的可靠性。可以为垃圾邮件和非垃圾邮件指定文件夹，对其进行手动扫描或按指定的时间间隔进行自动扫描。对这些文件夹中的所有邮件将作分析和检索，或者说 "贝叶斯学习"，以便新邮件能与其统计信息进行比较，来确定新邮件是否为垃圾邮件的可能性。然后可根据贝叶斯比较的结果增减邮件的SpamAssassin 分数。

启发式规则更新

每晚午夜时分检查启发式规则更新
若希望 SecurityGateway 于每晚午夜自动检查启发式规则更新，请选择该选项。

每隔 [XX]小时检查启发式规则更新
若希望 SecurityGateway 每隔若干小时而不只是简单地每天一次自动检查启发式规则更新，请选择该选项并指定数值。

不检查启发式规则更新
若不希望 SecurityGateway 自动检查启发式规则更新，请选择该选项。您仍可使用以下 *"点击此处检查..."*选项来手动检查更新。

运行 SA-Update 作为更新过程的一部分
如果您希望不仅能从 updates.spamassassin.org 获得更新，还能从 MDaemon Technologies 获得更新，请激活该选择框。该功能将确保您的 SpamAssassin 规则设置始终保持最新状态。默认情况下启用此项。

点击此处立即检查启发式规则更新
点击该链接手动检查启发式规则更新。

贝叶斯分类

启用"贝叶斯"分类
选中该复选框启用 SGSpamD 的贝叶斯分类系统。若希望根据邮件与当前已知贝叶斯统计信息的比较结果调整每封邮件的 SpamAssassin 分数，请使用该功能。

贝叶斯分类器在开始调整邮件的 SpamAssassin 分数前需要对垃圾邮件和非垃圾邮件的范例进行分析。这就是贝叶斯学习过程，通过这一过程，才能在进行贝叶斯比较时有充足的统计信息库供提取。一旦获得了这些供分析的邮件，贝叶斯学习系统即装备齐全，可以开始对每封邮件的 SpamAssassin 分数应用贝叶斯比较结果。通过不断分析更多的邮件，贝叶斯分类将随着时间的推移变得更为准确。

必须学习的非垃圾邮件：
这是指定为"非垃圾邮件"的邮件数目，贝叶斯分类器开始为邮件评分前必须对其进行分析。默认值为 200 封邮件。

必须要学习的垃圾邮件：
这是指定为"垃圾邮件"的邮件数目，贝叶斯分类器开始为邮件评分前必须对其进行分析。默认值为 200 封邮件。

贝叶斯学习

每晚午夜调度"贝叶斯"学习
若希望贝叶斯学习系统每日一次，从午夜开始，自动分析特定的垃圾邮件和非垃圾邮件文件夹中包含的邮件，请选择该选项。

每隔 [XX] 小时调度贝叶斯学习
若希望贝叶斯学习系统每隔指定的若干小时，而不是每晚午夜，自动分析特定的垃圾邮件和非垃圾邮件文件夹中包含的邮件，请选择该选项并指定数值。

不执行调度的贝叶斯学习
若不希望调度贝叶斯学习，请选择该选项。然而，您仍可随时点击下方的 *"单击此处立即执行贝叶斯学习"*链接手动启动贝叶斯学习过程。

到已知垃圾邮件目录（漏报）的路径：
该路径指向的文件夹包含指定的垃圾邮件。可以手动或使用自动贝叶斯学习选项自动地将垃圾邮件置于此处。

到非垃圾邮件目录（误报）的路径：
该路径指向的文件夹包含指定的非垃圾邮件。可以手动或使用自动贝叶斯学习选项自动地将非垃圾邮件置于此处。

垃圾邮件转发地址：
使用该文本框指定用户转发垃圾邮件的地址，以便贝叶斯系统能从中进行学习。SecurityGateway 使用的默认地址是 "SpamLearn[@AnySGDomain.com]"，但您可随意更改。必须通过 SMTP 从经 SMTP AUTH 验证过的会话处来接收发往该地址的邮件。不仅如此，该邮件必须作为 "message/rfc822" 类型的附件转发给上述地址。对任何其他类型的发往该地址的邮件不作处理。最后，当将地址输入该选项时，请只使用地址的邮箱部分 — 请勿包括 "@" 或域部分。例如："Spam"、"SpamLearn"、"SpamMail" 等等都为可接收的地址，能在该选项中使用。随后，邮件可转发至任意 SecurityGateway 域内的上述地址（例如 SpamLearn@example.com、SpamLearn@company.mail 等）。

非垃圾邮件转发地址：
使用该文本框指定用户转发非垃圾邮件的地址，以便贝叶斯系统能从中进行学习。SecurityGateway 使用的默认地址是 "NonSpamLearn[@AnySGDomain.com]"，但您可随意更改。必须通过 SMTP 从经 SMTP AUTH 验证过的会话处来接收发往该地址的邮件。不仅如此，该邮件必须作为 "message/rfc822" 类型的附件转发给上述地址。对任何其他类型的发往该地址的邮件不作处理。最后，当将地址输入该选项时，请只使用地址的邮箱部分 — 请勿包括 "@" 或域部分。例如："NonSpam"、"NonSpamLearn"、"GoodMail" 等等都为可接收的地址，能在该选项中使用。随后，邮件可转发至任意 SecurityGateway 域内的上述地址（例如 NonSpamLearn@example.com、NonSpamLearn@company.mail 等等）。

不学习大于 [XX] 字节的邮件
因为较大的邮件通常不是垃圾邮件，也因为对其进行分析需要执行大量处理操作，因此默认对超过 50,000 字节的邮件不作分析。根据您的选择，您可使用该选项调整大小值，或完全禁用该选项以分析任意大小的邮件并继续下一步配置。

点击此处立即执行贝叶斯学习
除了可能已设置的调度间隔外，可点击该链接随时手动启动贝叶斯学习过程。

自动贝叶斯学习

启用"贝叶斯"自动学习
使用自动贝叶斯学习，可以为合法（即非垃圾）邮件和垃圾邮件指定邮件评分阈值。自动学习将最终邮件得分低于非垃圾邮件阈值的任何邮件都视为非垃圾邮件，而将得分高于垃圾邮件阈值的任何邮件视为垃圾邮件。尽管该选项的使用应谨慎，但若您仔细地设置了阈值，自动学习会变得非常有用，这是因为它使得从数据库文件（参见下面的*贝叶斯数据库*）中删除的过期令牌能被自动替换。它能给予贝叶斯学习系统源源不断的新邮件供其学习，同时无需手动再培训以恢复过期令牌。

认为得分低于 [XX] 的邮件合法
邮件分数低于该值的邮件将归类为合法/非垃圾邮件供贝叶斯学习之用。

...只学习来自于域邮件服务器和已验证会话的非垃圾邮件
点击该选项，若希望仅将自动贝叶斯学习合法邮件应用于来自经验证的会话或域邮件服务器[66]的邮件。使用该选项时，来自非本地源的入站邮件无论其最终邮件得分多少，都不会用于贝叶斯学习，除非它们来自域服务器或已验证源。然而，您仍可手动复制任意合法邮件到上列指定的 "非垃圾邮件"文件夹，从而使系统也能学习这些邮件。

认为得分高于 [XX]的邮件为垃圾邮件
邮件分数高于该值的邮件将归类为垃圾邮件供贝叶斯学习之用。

...只从入站邮件中学习垃圾邮件
若希望只对入站邮件应用垃圾邮件的自动贝叶斯学习，请点击该选项。当使用该选项时，外发邮件无论其最终邮件得分多少，都不会用于贝叶斯学习。然而，您仍可手动将邮件置于上列 "垃圾邮件"文件夹。

贝叶斯数据库

启用贝叶斯自动令牌过期
该选项使得每当达到以下指定的令牌数时，贝叶斯系统能自动终止数据库令牌。设置令牌限额能防止贝叶斯数据库过大而减慢处理速度。

最大贝叶斯数据库令牌数：
这是所允许的最大贝叶斯数据库令牌数。当达到该令牌数时，贝叶斯系统删除最老的令牌，使令牌数降为该值的 75% 或 100,000 (取其中的较大值)。无论有多少令牌过期，令牌数决不会低于此二值中的较大值。请注意：150,000 个数据库令牌约为 8MB。

高级

最大邮件处理线程数 (1-6)：
使用该选项指定 SGSpamD 在任何时候能同时使用的邮件处理线程最大数量。可将该值设为 1 到 6 个线程。默认值为 4。

每个线程的最大 TCP 连接数 (10-200)：
这是任何时候每个邮件处理线程与 SGSpamD 所允许的最大 TCP 连接数。该值可设为 10-200。默认值为 200。

4.1.3 DNS 黑名单 (DNSBL)

DNS 阻止列表 (DNSBL)可用来防止垃圾邮件接近您的用户。该安全功能允许您指定若干个 DNS 阻止列表服务 (它们维持了中继垃圾邮件所知的服务器列表)，每次有人试图发送邮件至您的其中一个域，都将对该邮件进行安全性检查。若连接的 IP 已被这些服务中的任何一项列入阻止列表，那么该邮件将被拒绝，隔离，或者标记。

使用该功能可防止大多数垃圾邮件发送至您的用户。不过，一些站点会被错误地列入阻止列表。所以如果您使用该功能来彻底拒收来自于已列入阻止列表的 IP 地址的邮件，可能会引起一些麻烦。不过该功能还是值得使用的，尤其是与 SecurityGateway 其他具有垃圾邮件防护功能的选项结合使用，例如 URI 阻止列表，邮件评值，以及启发式和贝叶斯选项。

配置

启用 DNSBL 查询
该选项是对照 DNS 阻止列表的，用于检查入站邮件。SecurityGateway 将为发件服务器的 IP 地址◆◆询下方所列出的每一个 DNSBL 主机。如果主机以积极的结果回应查询，则表明此 IP 地址已列入阻止列表，将拒收、隔离、或者接受并标记该邮件，这取决于您在下方所指定的选项。默认情况下启用此项。

若已列出了邮件的发件服务器：

...拒收邮件
如果您使用了此选项，那么在 SMTP 会话过程中，将拒收 IP 地址已列入阻止列表的入站邮件。或者，在拒收邮件的过程中，SecurityGateway 可以使用一个与阻止列表主机相关联的自定义反应来告知连接服务器为何邮件会被拒收，而不是使用传统的 "用户未知" 反应。在创建主机条目时，可通过使用下方的 *"邮件"* 选项来指定每一个 DNSBL 主机的相关反应。通过启用 "当拒收一封返回的是 '邮件' 而不是 '用户未知' 的邮件" *这个选项*，您可配置 SecurityGateway 让其发送此类响应而不是传统的 "用户未知" 响应。

...隔离邮件
如果您希望隔离来自于 DNS 已列入阻止列表的 IP 地址的邮件，请选择此选项。

...接受邮件
根据默认，将接受来自于已列入阻止列表地址的邮件，随后可将其标记为垃圾邮件，在主题行上添加一个标记，且/或调整其邮件分值。使用该选项可允许邮件服务器或者用户根据 SecurityGateway 的 DNSBL 查询结果自己来过滤邮件。

...用 [文本] 标记主题
当邮件来自于一个已列入阻止列表的 IP 地址时，如果您希望在邮件的主题报头上加一些内容，启用此选项并指定一些文本。根据默认该选项是禁用的。如果将其开启，根据默认 "*** 垃圾邮件 ***" 将加入主题，不过如果您可选择对其进行编辑。

您可在 SecurityGateway 中的多个其他地方选择添加文本到主题报头。例如，邮件分数 143 和 URI 阻止列表 (URIBL) 137 页面均有此选项。当这些选项中的指定文本相匹配时，该文本在邮件主题中只添加一次，即使该邮件满足每个选项下的条件。然而，如果您在一处或多处更改了文本，则同样也会添加该定制文本。因此，举个例子，若您在所有这三个选项下都将文本设置为 "*SPAM*"，则该文本在主题中只会添加一次，而不管邮件是否匹配多个选项下的条件。不过，如果您将 DNSBL 可选文本改为 "*DNS 阻止列表*"，在此选项和其他选项下邮件均符合标准，那么主题中将同时添加 "*垃圾邮件*" 和 "*DNS 阻止列表*"。

...向邮件总值添加 [XX] 点数
如果邮件已列入 DNS 阻止列表，使用此选项在邮件分数上加上指定的分值。默认启用该选项，并向邮件总值添加 5.0 个点数。

即使 SecurityGateway 配置为接受邮件而不是拒绝或隔离邮件，但若邮件最终得分足够高，该邮件仍可能被拒绝或隔离，这取决于

其他安全[124]选项和邮件评分[143]页上选项的配置。

例外

排除来自被列入允许列表的发件人的邮件
默认情况下，如果邮件源自允许列表[212]的发件人，该邮件则免于 DNSBL 查询。即使发件人已列入允许列表，如果您还是希望查询 DNSBL 主机，请禁用此选项。

排除来自经身份验证会话的邮件
当一封邮件的会话已通过验证，若您希望将邮件排除于 DNSBL 查询之外，请使用此选项。默认情况下启用此项。

排除来自域邮件服务器的邮件
来自于域邮件服务器[66]的邮件总是无需受到 DNSBL 主机查询。

DNSBL 主机（所有域）

新主机：
要向 DNSBL 主机列表中添加新主机，请在此输入需要查询的主机（例如，zen.spamhaus.org），在下方添加相应的*"邮件"*，然后点击*"添加"*。

邮件：
这是一封与上方输入的*新主机*相对应的邮件，在查询该主机时，SecurityGateway 找到了一个已列入阻止列表的 IP 地址，那么相应的邮件将记录到日志中。若您拒收了来自于已列入阻止列表地址的邮件，在 SMTP 会话过程中该邮件会返回连接服务器，并且已启用下方*"当拒收一封返回的是'邮件'而不是'用户未知'邮件"*选项。您可使用此邮件中的 IP 宏，若您希望在其中包含已列入阻止列表的 IP 地址。

添加
输入*"新主机"*以及相应的*"邮件"*后，点击此按钮将其加入 DNSBL 主机列表。

删除
若您希望从 DNSBL 主机列表中删除一个条目，将其选中然后点击此按钮。

找到第一个列出该连接 IP 的主机后停止 DNSBL 查询
很多时候一封邮件的报头包含了多个 IP 地址，而且需要为这些地址查询多个 DNSBL 主机。根据默认，一旦发现一个已列入阻止列表的 IP 地址，SecurityGateway 将停止为任何给定的邮件查询 DNSBL 主机。即使找到了一个已列入阻止列表的地址，您若还是希望继续为所有地址和 DNSBL 主机执行查询操作，可禁用此选项。

当拒收一封返回的是"邮件"而不是"未知用户"邮件
当找到一个已列入阻止列表的 IP 地址时，若您将 DNSBL 选项配置为*"...拒收邮件"*，根据默认上方所列出的与 DNSBL 主机相对应的短*消息*将记录到日志日志文件并在 SMTP 会话过程中返回到连接服务器。若您还是希望使用标准的"用户未知"邮件，请不要勾选此选项。

高级（所有域）

在已收集的邮件中检查“已收到”的报头
根据默认，SecurityGateway 只会为真正连接到 DNSBL 主机的 IP 地址并试图投递一封邮件的主机的 IP 地址提供 DNSBL 主机查询。若您希望对在邮件的“已接收”报头中找到的 IP 地址也执行 DNSBL 查询，请勾选此选项。

只检查这个有很多“已收到”的报头（0=全部）
当您配置完 SecurityGateway，让其为已列入阻止列表的 IP 地址检查“已接收”报头，若您希望限制要被检查的报头数，请在此选项中输入一个数值。若您希望检查所有的报头，请使用“0”。

跳过这么多最新的“已接收”报头（0=没有）
当您配置完 SecurityGateway，让其为已列入阻止列表的 IP 地址检查“已接收”报头，若您希望跳过一定数量的最新报头，请在此选项中输入一个数值。根据您特别的邮件系统配置，有时候最近的报头中将包含可信的主机或者网络上其他电脑的 IP 地址，它们无需受到任何阻止列表的检查。若您不希望跳过任何最近的报头，请在此选项中使用“0”。

跳过这么多最旧的“已接收”报头（0=没有）
当您配置完 SecurityGateway，让其为已列入阻止列表的 IP 地址检查“已接收”报头，若您希望跳过一定数量的最旧报头，请在此选项中输入一个数值。最旧的报头常常不包含任何要检查的相关地址，因为它们是由发件人的内部邮件服务器添加的，或者伪造成看似合法的外观。若您不希望跳过任何最旧的最近报头，请在此选项中使用“0”。

例外 - 域

当配置这些设置时，如果您在页面顶部的*“针对域：”*下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。点击相应域的*“查看/编辑”*链接来查看或编辑其 DNS 阻止列表设置，或者点击*重置*，将域设置重置为默认的全局值。

4.1.4 URI 阻止列表 (URIBL)

URI 阻止列表 (URIBL) 是实时的阻止列表，用于根据邮件正文中找到的统一资源标识符（通常为域名或网站）阻止或标记垃圾邮件。也称为垃圾邮件 URI 实时阻止列表 (SURBL)，URIBL 与 DNS 阻止列表 134 的不同之处在于：它们不是用于根据报头的内容或连接的 IP 地址识别垃圾邮件。相反，URIBL 根据邮件内容阻止垃圾邮件。有关 URIBL 工作方式的详尽信息请访问 www.surbl.org。

配置

启用 URIBL 查询
默认情况下，SecurityGateway 对邮件执行 URIBL 查询。若不希望执行该查询，请取消选中该选项。

若邮件包含所列 URI：

...拒收邮件
若希望在 SMTP 处理过程中当发现邮件包含列入阻止列表的 URI 时拒绝该邮件，请选择该选项。大多数情况下，这并非推荐的选项，因为仅仅在邮件正文中引用列入阻止列表的 URI 不能保证该邮件本身即是垃圾邮件。

...隔离邮件
若希望当发现邮件中包含列入阻止列表的 URI 时隔离该邮件，请选择该选项。

...接受邮件
如果您希望当发现邮件中包含列入阻止列表的 URI 时接受该邮件，但将其标识为垃圾邮件，为主题行添加标记，和/或调整邮件分数，请选择该选项。使用该选项允许邮件服务器或收件人根据 SecurityGateway 的 URIBL 查询结果过滤邮件。这是默认选项。

...用 [文本]标记主题
若希望当发现邮件中包含列入阻止列表的 URI 时，为该邮件主题报头添加起首文本，请启用该选项并指定相应文本。若启用，添加到主题的默认文本是："*** SPAM ***"。默认情况下，禁用该选项。

> 您可在 SecurityGateway 中的多个其他地方选择添加文本到主题报头。例如，DNS 阻止列表 (DNSBL) 134 和邮件评分 143 页也有该选项。当这些选项中的指定文本相匹配时，该文本在邮件主题中只添加一次，即使该邮件满足每个选项下的条件。然而，如果您在一处或多处更改了文本，则同样也会添加该定制文本。因此，举个例子，若您在所有这三个选项下都将文本设置为 "*SPAM*"，则该文本在主题中只会添加一次，而不管邮件是否匹配多个选项下的条件。但是，如果您将 URIBL 可选文本更改为 "*URI blocklisted*"，且邮件匹配该选项及其他选项下的条件，则主题中将同时添加 "*SPAM*" 和 "*URI blocklisted*"。

...在邮件得分上添加由 URIBL 引擎返回的分数
默认情况下，当 URIBL 查询指示邮件包含列入阻止列表的 URI 时，将在邮件分数上添加与查询到的 URIBL 主机相关的分数。若不希望根据 URIBL 查询结果调整邮件分数，请取消选中该选项。

> 即使 SecurityGateway 配置为接受邮件而不是拒绝或隔离邮件，但若邮件最终得分足够高，该邮件仍可能被拒绝或隔离，这取决于其他安全 124 选项和邮件评分 143 页上选项的配置。

例外

排除来自被列入允许列表的发件人的邮件
默认情况下，如果邮件源自允许列表 212 的发件人，该邮件则免于 URIBL 查询。若希望在发件人列入允许列表的情况下仍查询 URIBL 主机，请禁用该选项。

排除来自经身份验证会话的邮件
若希望当 SMTP 会话通过身份验证时使其上的邮件免于进行 URIBL 查询，请选中该选项。该选项默认为禁用。

排除来自域邮件服务器的邮件
默认情况下，对入站邮件和来自域邮件服务器 66 的邮件都执行 URIBL 查询。若希望使来自域邮件服务器的邮件免于进行 URIBL 查询，请选中该复选框。

URI 阻止列表（所有域）

该部分列出了 SecurityGateway 将查询的 URIBL 主机。

新建
要添加新的 URI 阻止列表，请单击*新建*按钮。这会打开 URI 阻止列表编辑器 139（如下）。

编辑
要编辑某个 URI 阻止列表，请选择希望编辑的条目并点击*"编辑"*按钮。这会打开该条目的 URI 阻止列表编辑器 139。

删除
要删除 URI 阻止列表，请选择希望删除的条目并单击*删除*按钮。

例外 - 域

当配置这些设置时，如果您在页面顶部的*"针对域："*下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。点击相应域的*"查看/编辑"*链接以查看或编辑其 URI 阻止列表设置，或点击*"重置"*将域设置重置为默认全局值。

URI 阻止列表编辑器

通过在 URI 阻止列表页面上单击*新建*或*编辑*可打开该阻止列表编辑器，它用于添加新的 URI 阻止列表并编辑现有的阻止列表。

保存与关闭
添加或更改阻止列表的任何设置后，单击该按钮可保存更改并关闭编辑器。

关闭
点击该按钮可关闭编辑器，而不保存您所做的任何更改。

URI 阻止列表

启用此 URI阻止列表查询
使用该选项启用或禁用给定的 URI 阻止列表。若取消选中某一条目的这一复选框，该条目不会从列表中删除，但 SecurityGateway 将不会查询相应的 URI 阻止列表。

URIBL 名称：
这是要查询的特定 URI 阻止列表名称。

主机名或 IP：
这是与 URI 阻止列表条目对应的主机名或 IP 地址，SecurityGateway 在检查邮件中找到的 URI 时将查询该阻止列表。

分数：
该 URIBL 分数是与 URIBL 关联的指定数值，当查询结果为在邮件中找到列入阻止列表的 URI 时会用到。在最终邮件分数 143 上将添加该分值，除非在 URI 阻止列表页面上已禁用*...在邮件得分上添加由 URIBL 引擎返回的分数*选项。

位掩码：
位掩码值用于标识当多个列表合并为单个位掩码列表时要查询的列表或数据源。在 *multi.surbl.org* 中专门整合了所有的 SURBL 数据源。更多相关信息，请参见：www.surbl.org。若所查询的 URIBL 只包含单个列表的信息，可使用 "0"。

执行查询之前解析 URI的 IP 地址
若希望在查询 URI 阻止列表之前解析或查找邮件中所含 URI 的 IP 地址，请使用该选项。类似于 DNSBL[134]，某些 URIBL 会存储 IP 地址，但它们存储的是邮件中所含 URI 的地址，而非发送该邮件的邮件服务器地址。

4.1.5 灰名单

灰名单是一项对抗垃圾邮件的技术，它通过告知发送方的邮件服务器出现了一个暂时性的错误，必须以后重新发送。理论上来说，垃圾邮件工具基本上不会重试投递，而合法的邮件服务器会。使用了这项技术，当一封邮件来自于一个未被列入允许列表的发件人或者先前是未知的发件人，那么将把该邮件的发件人、收件人和发件服务器的IP 地址记录到日志，然后在 SMTP 会话过程中将暂时拒收此邮件。此外，任何超出指定的分钟数的未来投递尝试都将被暂时拒收。因为如果一封邮件被拒收，垃圾邮件发送者一般不会做进一步投递尝试，那么灰名单可以缩短您的用户接收垃圾邮件的时间。即使垃圾邮件制造者以后试图重新投递，但到那时垃圾邮件制造者很可能已被识破并将被其它反垃圾邮件选项 (例如 DNS 阻止列表)成功拦截。

尽管灰名单有能力减少垃圾邮件的数量，不过值得注意的是，在减少垃圾邮件数量的同时，它也中继了合法邮件甚至是重要邮件。不过，合法邮件在灰名单周期过期后仍会进行投递，并且对于同一个服务器/发件人/收件人组合不会再执行中继操作，除非在指定的天数内发件人未将另一封邮件发送至收件人。另外一点值得注意的是，当邮件被中继时，您无从得知发件服务器需要等待多久才能进行重试投递尝试。可以故意以一个暂时性错误代码拒收邮件，将使得该邮件的中继时间只有几分钟或者有一整天那么长。由于总有这样那样的潜在问题与灰名单相关联，所以在 SecurityGateway 中根据默认，该功能已禁用。不过，还指定了一些选项用来处理这些潜在问题。

首先，有一些发件域是由多个邮件服务器汇集而成的，用来发送出站邮件。由于每一次投递尝试可以使用一个不同的邮件服务器，每一次尝试可视作是与灰名单引擎的一次新连接。这可以大大缩短邮件通过灰名单的时间，因为每一个尝试都会列入灰名单，就好像它们都是分离的邮件而不是重试先前的邮件。使用发件人策略框架 (SPF)查询选项，向发件域发送谁发行了它们的 SPF 数据，这个问题便得以解决。此外，有一个选项可完全忽略发件邮件服务器的 IP 。使用该选项会降低灰名单的效率，不过可以解决多个服务器的问题。

其次，灰名单一般要负担一个很大的数据库，因为它必须跟踪每一个入站连接。SecurityGateway 通过将灰名单置于 SMTP 处理过程的较后位置，从而将跟踪连接的需求减到最小。这就允许 SecurityGateway 的很多其他选项在到达灰名单这个步骤之前就拒收邮件。这样做的结果是，大大缩小了灰名单数据库的尺寸并且造成较小的实际操作上的影响。

最后，还提供了一些选项来将灰名单对于合法邮件的影响最小化，例如将邮件排除在灰名单以外的选项，条件是邮件来自于列于允许列表的发件人或者来自于已验证会话。此外，来自于您其中一个域邮件服务器的邮件总是不受灰名单的影响。

有关灰名单的更多信息，请访问：

http://en.wikipedia.org/wiki/Greylisting

配置

启用灰名单
点击此选项来启用灰名单功能。根据默认，灰名单已被禁用。

以暂时性的错误来延缓初始的传输尝试 [xx]分钟
使用此选项来指定继初始投递尝试后，每一个服务器/发件人/收件人组合 (例如："三位字节")将列入灰名单的分钟数。在这段时间里，任何以此相同三位字节所进行的投递尝试将以暂时性错误代码的方式被拒收。过了指定的分钟数后，将不再对此三位字节执行灰名单中继操作，除非灰名单数据库记录过期。该选项的默认值是 15 分钟。

在 [xx]天之后终止不用的灰名单数据库记录
一旦列入灰名单的三位字节超过了初始的灰名单周期，那么将不再对其执行进一步的投递中继，除非在这个天数内没有发送过与此三位字节记录相匹配的邮件。例如，若该值设为 10 天，则要求至少每 10 天收到一封与同一个服务器/发件人/收件人组合相匹配的邮件，这样便可不再中继。不过，如果在那段时间里没有邮件发送，那么该记录将会过期。此三位字节在免受进一步中继之前，它必须经历另一个灰名单周期。一个记录在其到期之前必须有一些天保持不用的状态，此默认时间为 10 天。

列灰名单时忽略 IP 地址 (仅使用 MAIL & RCPT 值)
若您不希望将发件服务器的 IP 地址用作灰名单的其中一个参数，请点击此选择框。这将解决由多个服务器而引起的潜在问题，不过这将降低灰名单的效率。默认情况下，禁用该选项。

忽略通过 SPF 处理的用于连接的 IP 地址
使用了此选项后，当发件服务器通过 SPF 处理 151 时，只有发件人和收件人用于灰名单，IP 地址被忽略。默认情况下启用此项。

例外

排除来自被列入允许列表的发件人的邮件
根据默认，来自于允许列表 212 的发件人的邮件排除在灰名单之外—不会中继这些邮件的投递。如果您不希望将已列入允许列表的收件人排除在灰名单之外，请清理该选择框。

排除来自经身份验证会话的邮件
根据默认，来自于已验证会话的阿邮件不受灰名单的限制。若会话已通过验证，您仍不希望将邮件排除在灰名单之外，请清理此选择框。

排除来自域邮件服务器的邮件
来自于域邮件服务器 66 的邮件总排除在灰名单之外。

例外 - 域

当配置这些设置时，如果您在页面顶部的 *"针对域:"* 下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。点击 *"查看/编辑"* 相应域的链接来查看或编辑其灰名单设置，或者点击 *"重置"*，将域设置重置为默认的全局值。

4.1.6 反向散射保护

反向散射

“反向散射”表示用户接收到他们从未发出过的邮件的响应邮件。当病毒发送的垃圾邮件或邮件中包含伪造的“返回路径”地址时会发生反向散射。因此，当其中一封邮件被收件人服务器拒收时，或如果收件人使用自动应答程序或“外出”/假期邮件与其帐户关联，响应邮件随之将指向伪造的地址。这会导致海量的伪造投递状态通知 (DSN) 或自动应答邮件撑爆用户的邮件箱。另外，垃圾邮件发送者和病毒编写者会经常利用该现象，有时使用它对邮件服务器启动拒绝服务 (Denialof Service, DoS) 攻击，造成从世界各地的邮件服务器接收大量无效的邮件。

反向散射保护

为了与反向散射对抗，SecurityGateway 的反向散射保护 (BP)功能使用了私钥散列法生成并插入一个特殊的时间敏感代码至用户外发邮件的“返回路径”地址中，从而可以帮助确保您的域仅收到合法的投递状态通知和自动应答邮件。然后，当其中一封邮件遇到投递问题被弹回，或收到带有mailer-daemon@...”或者 NULL 反向路径的自动回复时，MDaemon 将检测到特殊代码并知道这是由您的联系人所发邮件的真实自动回复。若邮件不包含特殊代码或者代码已过期，将会被记录下来并且可拒收。

配置

启用反向散射保护
欲启用反向散射保护，请点击该选择框。SecurityGateway 随之将开始生成并插入一个特殊的代码至所有出站邮件的返回路径，并且它将在所有已返回的邮件中搜索该代码。根据默认，反向散射保护已禁用。

如果禁用该选项，SecurityGateway 将不会在外发邮件中插入特殊的反向散射保护代码。不过，它仍将继续检查入站的 DSN 及自动应答邮件以确保不会错误地拒收任何带有正确代码的接收邮件。

拒收验证反向散射保护失败的邮件
如果要拒收 BP 验证失败的 DSN 或其他自动应答邮件，可以点击此选择框。带有“mailer-daemon@...”或“NULL”反向路径的邮件如果不包含特殊代码或超过代码的七天有效期，则无法通过 BP 验证。由于反向散射保护坚实的可靠性，不存在误报或“灰色区域”——邮件要么有效，要么无效。因此配置 SecurityGateway 拒收无效邮件非常安全，只要确保所有联系人的外发邮件中都包含特殊的 BP 代码。即使您选择不拒收验证失败的邮件，但在所有情况中，BP 验证的结果都会被记录到日志文件中。

启用反向散射保护后，将其设置为拒收未通过 BP 验证的自动应答邮件前应等待一周左右时间。因为在此期间，您仍可能在激活 BP 前接收到发出邮件的 DSN 或自动应答。如果在此期间将 BP 配置为拒绝无效邮件，则这些合法的应答邮件将被错误地拒收。大约一周后开始拒收未通过验证的邮件会比较安全。当您创建一个新的 BP 密钥而没有选择使用*保留先前的反向散射保护加密密钥[xx]天*选项时，相同的警告同样适用。

点击此处将立即生成一个新的反向散射保护加密密钥
点击此选项将手动地生成新的反向散射保护密钥。如果启用了下方的 *"保留先前的反向散射保护加密密钥 [xx] 天"*这个选项，那么在该选项的指定的天数里，包含由先前密钥所生成的代码的邮件会保持有效。

例外

排除发自被列入全局允许列表的 IP 地址和主机的邮件
根据默认，若启用了反向散射保护，来自全局被列入允许列表[212]的 IP 地址和主机的所有邮件都不受反向散射保护的限制。如果您希望这些已列入允许列表的 IP 和主机也要遵守这些限制的话，请清除此选择框。

排除来自经身份验证会话的邮件
如果一封入站邮件来自于一个已验证的会话，那么根据默认，它将排出于反向散射保护的限制之外。如果您希望这些限制同样应用于已验证的会话，请不要勾选此框。

排除来自域邮件服务器的邮件
根据默认，如果启用反向散射保护，来自于其中一个域邮件服务器[66]的入站邮件不受反向散射保护的限制。如果您不希望将域邮件服务器排除在反向散射保护检查的范围之外，请清除该选择框。

邮件返回路径签名

每隔 [xx] 天创建一个新的反向散射保护加密密钥
根据默认，每七天生成一个新的反向散射保护加密密钥。该密钥将用来给所有新的出站邮件生成 BP 代码。

保留先前的反向散射保护加密密钥 [xx] 天
根据默认，在生成新的加密密钥后，SecurityGateway 将继续验证含有先前加密密钥所生成的反向散射代码的邮件，这个验证过程将持续七天。从而确保有效邮件不会因为生成新的密钥而被不小心拒收。不推荐禁用此选项（请查看位于 *上述拒收未通过反向散射保护验证的邮件* 选项底下的警告）。

不将返回路径签名邮件发送到下方列出的 IP 地址或域
使用此选项可以指定任何 IP 地址和域名来免于"反向散射保护"的返回路径签名。

4.1.7 邮件评分

SecurityGateway 在处理邮件的时候，会根据它所执行的一系列测试为每封邮件计算邮件总值。该总值是一个有效的"垃圾邮件总值"，用于决定一封邮件为垃圾邮件的可能性。启发式与贝叶斯[129]，DNSBL[134]，DKIM 验证[154]，与许多其他的安全[124]功能都可以选择性地进行设置以修改邮件总值。使用该页的选项来指定当邮件的总值超过某个阈值时会执行的操作。您可以设置阈值以将邮件标记为垃圾邮件，隔离邮件，或在 SMTP 会话中拒收它们。您还可以对 SecurityGateway 进行设置，以让它将那些来自列于允许列表的发件人与经验证的会话的邮件或外发邮件从邮件评值限制中排除。邮件评值选项既可以进行全局设置，也能针对特定的域设置。

配置

根据最终邮件总值执行操作
默认情况下，SecurityGateway 将为每一封邮件指定一个总值并根据该值，依照以下指定的评值阈值采取行动。如果您不希望根据邮件总值采取任何行动，清除该复选框。

总值大于或等于 [xx]时拒收邮件
默认情况下，任何最终总值大于或等于 12.0 的邮件将在 SMTP 会话中被拒收。如果选中该选项，您可以调整这个值，如果您不希望任何邮件因为其总值而被拒收，您可以完全禁用该选项。

总值大于或等于 [xx]时隔离邮件
默认情况下，会隔离邮件评值大于或等于 5.0 的邮件。该值可以进行调整，如果您不希望根据邮件的邮件总值隔离它们，您可以完全禁用该选项。如果您同时还在使用以上的*"总值大于或等于 [xx] 时拒收邮件"*选项，那么会隔离邮件评值介于该隔离阈值与以上的拒收阈值间的邮件。会拒收邮件评值大于或等于该拒收阈值的邮件。

总值大于或等于 [xx]时向邮件添加主题标签
当最终总值大于或等于该值时，如果您希望向邮件主题添加一些文本，请单击该选项。默认值是 5.0，但是默认情况下禁用该选项。

主题标签：
当启用以上的*"向邮件添加主题标签……"*选项，在邮件总值大于或等于要求的阈值时，这就是将添加至邮件主题的文本。该选项将添加的默认文本是："*** SPAM ***"。（"*** 垃圾邮件 ***"）。

SecurityGateway 内还有一些其他位置，供您可以有选择性地将文本添加到 "主题"报头。例如，DNS 阻止列表 (DNSBL)134与 URI 阻止列表 (URIBL)137页面也有该选项。当这些选项中的指定文本相匹配时，该文本在邮件主题中只添加一次，即使该邮件满足每个选项下的条件。然而，如果您在一处或多处更改了文本，则同样也会添加该定制文本。因此，举个例子，若您在所有这三个选项下都将文本设置为 "SPAM*"，则该文本在主题中只会添加一次，而不管邮件是否匹配多个选项下的条件。但是，如果您将 URIBL 的可选文本更改为 "URIblacklisted*"（"URI阻止列表*"）并且它在该选项与其他选项下满足了条件，那么就会向主题添加 "SPAM*"（"垃圾邮件*"）与 "URIblacklisted*"（"URI阻止列表*"）两种文本。

例外

排除来自被列入允许列表的发件人的邮件
默认情况下，邮件来自列于允许列表212的发件人时，会将它们从邮件评值限制中排除。如果您不希望将列于允许列表的发件人从邮件评值中免除，请清除该复选框。

排除来自经身份验证会话的邮件
默认情况下，任何通过已验证的 SMTP 会话的外发邮件，会从邮件评值限制中排除。如果您不希望排除这些邮件，请不要勾选该复选框。

排除来自域邮件服务器的邮件
如果您希望将所有来自您域邮件服务器的邮件从邮件评值限制中排除，请点击该复选框。默认情况下，禁用该选项。

例外 - 域

当配置这些设置时，如果您在页面顶部的 *"针对域："* 下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。在相应的域中点击 *"查看/编辑"* 链接以查看或者编辑其邮件评值设置，或点击 *"重置"* 来将域的设置重置回默认的全局值。

4.1.8 数据查询服务 (DQS)

数据查询服务 (DQS) 是一套 DNSBL[134]，它们实时进行更新并由 Spamhaus Technology 运营，由此来阻止超过 99% 的由电子邮件带来的威胁。DQS 需要由 Spamhaus Technology 提供的有效订阅和使用密钥。要使用 DQS 服务：

1. 激活您的数据查询服务的免费试用。
2. 点击 **"启用 Spamhaus 数据查询服务 (DQS)"**。
3. 输入您的 **Spamhaus DQS 密钥**。
4. 点击 **"保存"**。

4.1.9 Abusix

Abusix Mail Intelligence™ 是一套实时的 DNSBL[134]，其设计旨在阻止随邮件携带的威胁。Abusix Mail Intelligence 需要 Abusix 提供的有效订阅和使用密钥。要使用 Abusix 服务：

1. 转至 Abusix 并注册新账户.
2. 在 SecurityGateway 中，点击**启用 Abusix Mail Intelligence**。
3. 输入您的 **Abusix 密钥**。
4. 点击 **"保存"**。

要了解有关 Abusix Mail Intelligence 的更多信息，请参阅 Abusix 文档页面。

4.2 反病毒

安全[124]菜单下的反病毒区段中包含能够帮您识别受到病毒感染的邮件并防止其到达您用户的选项。在反病毒部分下共有两个项目：

病毒扫描[146]——为了给用户提供一个广泛的病毒保护，SecurityGateway 提供两款反病毒引擎：Clam AntiVirus (ClamAV™) 和 IKARUS Anti-Virus。ClamAV 是专门为邮件网关设计的开源 GPL)防病毒工具包。IKARUS Anti-Virus 提供可靠的保护来使用户免受恶意软件和潜在敌对程序的侵扰。它整合了传统的病毒防护方法和最新的前瞻性技术。SecurityGateway 还包含 爆发保护[126]，为您提供了抵御病毒爆发的传统保护层。

配置更新[148]— 因为病毒威胁可能出现得很快，若使用了过时的病毒特征数据库，那么很可能遗漏病毒。因此，定期地进行病毒特征更新是非常重要的。使用配置更新页面上的选项，让 SecurityGateway 自动检查病毒特征更新，强制其对每一个更新进行快速检查，然后查看反病毒更新日志。

4.2.1 病毒扫描

为提供周密的病毒防护，SecurityGateway 支持两种反病毒引擎：Clam AntiVirus (ClamAV™) 和 IKARUS Anti-Virus。ClamAV 是专门为邮件网关设计的开源 GPL)防病毒工具包。IKARUS Anti-Virus 提供可靠的保护来使用户免受恶意软件和潜在敌对程序的侵扰。它将传统的反病毒防护方式和最新的前瞻式技术结合在一起。SecurityGateway 还包含 "爆发保护[126]"，为病毒爆发又提供了一个额外的保护层。

配置

启用病毒扫描
SecurityGateway 中默认启用病毒扫描。如果不想扫描邮件以查找病毒，请清除此复选框。

如果反病毒引擎确定邮件已被感染：
使用该选项指定当发现邮件包含病毒时要执行的操作。

若已启用下面的 *"尝试清理被感染的邮件"*选项，SecurityGateway 将首先试图清理受感染的邮件 (即清除病毒)，而不是立即拒绝或隔离邮件。若清理成功，则接受并投递邮件。若邮件无法清理，则拒绝或隔离邮件。

...拒收邮件
选择该选项时，若在 SMTP 会话期间发现邮件包含病毒，则拒绝该邮件。这是默认选项。

...隔离邮件
若希望将被感染的邮件置于管理员隔离队列[256]而不是拒绝它们，可选择该选项。

隔离无法扫描的邮件
如果希望隔离反病毒引擎由于某些原因无法扫描的邮件，可点击该选项。这类邮件的一个典型例子是带有受密码保护的压缩附件的邮件。当禁用该选项时，无法扫描的邮件将按正常方式投递。默认情况下启用此项。

如果一个反病毒引擎扫描成功，则允许邮件通过
如果至少有一个防病毒引擎可以成功扫描邮件，要是您希望允许邮件通过，请选中此框。否则，如果其中任何一个引擎都无法成功扫描邮件，则将其隔离。

排除下方列出的文件
使用此选项来定义您希望从 *"隔离无法扫描的邮件"*这个限制中免除的特定文件或文件类型。允许文件掩码和通配符，例如：*.zip、secret?.zip、*.doc? 等。

尝试清理被感染的邮件
默认情况下，SecurityGateway 将首先试图从受感染的邮件中清除病毒（即"清理邮件"），而不是立即拒绝或隔离邮件。若清理成功，则正常投递该邮件。若邮件无法清理，则拒绝或隔离该邮件，这取决于以上所选择的选项。若不想尝试清理受感染的邮件，请清除该复选框。在这种情况下，将立即拒绝或隔离受感染的邮件。

将文档中包含宏的附件标记为病毒
使用此项可在病毒扫描期间检测文档中的宏。

例外

不扫描来自被列入允许列表的 IP 地址的邮件
如果您希望在邮件来自已允许 IP 地址[217]时使这些邮件免于病毒扫描，请启用此项。

不扫描来自域邮件服务器的邮件
若希望使来自域邮件服务器[66]的邮件免于病毒扫描，请启用该选项。

不扫描来自下列电子邮件地址的邮件
如果您希望邮件来自这些特定的发件人时，使邮件免于病毒扫描，请使用此项。

病毒扫描引擎（所有域）

使用 ClamAV 引擎来扫描邮件
默认情况下，SecurityGateway 将使用 ClamAV 防病毒引擎扫描邮件中的病毒。若不想使用 ClamAV 引擎扫描邮件，请清除该复选框。

使用 IKARUS Anti-Virus 引擎来扫描邮件
默认情况下，SecurityGateway 将使用 IKARUS 反病毒引擎来扫描邮件中的病毒。如果您不想使用 IKARUS 反病毒引擎来扫描邮件，请清除该复选框。

同时启用这两个选项意味着 SecurityGateway 将对每封邮件扫描两次 - 每个引擎一次。这就提供一个额外的保护层，因为一个引擎可能遗漏的病毒，另一个引擎却能识别出来。

例外 - 域

当配置这些设置时，如果您在页面顶部的 *"针对域:"* 下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。请点击相应域的 *"查看/编辑"* 链接以查看或编辑其病毒扫描设置，或点击 *"重置"* 将域设置重置为默认全局值。

4.2.2 配置更新

因为病毒威胁可能出现得很快，若使用了过时的病毒特征数据库，那么很可能遗漏病毒。因此，定期地进行病毒特征更新是非常重要的。使用此页面上的选项，让 SecurityGateway 自动检查病毒特征更新，强制其对每一个更新进行快速检查，然后查看反病毒更新日志。**注意：这些选项仅适用于 Clam AV 引擎。IKARUS Anti-Virus 引擎每 10 分钟执行一次更新检查。**

病毒更新

启用自动病毒特征更新
使用该选项来配置 SecurityGateway，以自动地定期检查已更新的ClamAV 病毒特征。您可以选择每一小时或每天自动地检查更新。根据默认，已启用自动更新功能。

按小时 — 在整点后 [xx] 分钟
默认情况下，SecurityGateway 依照此选项中所指定的整点后的特定分钟数，每小时检查一次已更新的 ClamAV 病毒特征。例如，如果您在此选项中使用了 "29"，那么执行每小时检查的时间将为1:29，2:29，以此类推。点击 *"生成随机时间"* 链接，用来为此选项生成一个随机的值。许多系统更新检查都定于很常见的时间，比如一个小时的头部或者尾部 (例如：1:00，1:30 等等)，那么选择一个随机时间可以潜在地加快您的更新检查速度，因为在其他时间里，系统较为畅通。

每天 — 在 [xx:xx] 时刻
若您希望每天检查一次已更新的病毒特征，请使用此选项，并在选项中指定时间。时间必须指定为 24 小时制格式。例如，如果您在此选项中使用了 "13:05"，那么每天的检查将于下午 1:05 执行。点击 *"生成随机时间"* 链接，用来为此选项生成一个随机的值。许多系统更新检查都定于很常见的时间，比如半夜 (例如 00:00)。选择一个随机时间可以潜在地加快您的更新检查速度，因为在其他时间里，系统较为畅通。

点击此处，立即对更新的病毒签名执行强制检查
点击该链接，让 SecurityGateway 立即检查已更新的病毒特征。立即检查操作将与您已配置的如下自动更新检查中的任意一个共同执行。

点击此处查看 ClamAV 的更新日志文件
点击此链接来查看 Clam AntiVirus 的更新日志。

点击此处来查看 IKARUS Anti-Virus 更新日志文件。
点击此链接来查看 IKARUS Anti-Virus 的更新日志。

4.3 反欺诈


安全性 菜单下的反诈骗部分包含了能够帮助您识别来自于伪造或是 "诈骗" 地址的邮件的工具。该部分下共列出了反诈骗邮件的六大功能：

反向查询[149] — 使用这些查询后，您可以查看发件人的域是否真实存在，以及发送方服务器的 IP 地址是否与该域相关。

发件人策略框架 (SPF)[151] — SPF 是一个开放标准，用来识别电子邮件中的伪造发件人地址。它尤其保护 SMTP 信封发件人地址或返回路径中的域。它通过检查域中用于 SPF 策略的 DNS 记录以精确地查出哪台邮件主机可以代表域发送邮件，从而做到如上所述。如果域有 SPF 策略而发件主机并没有列于该策略下，那么您就可以知道该地址是伪造的。

DKIM 验证[154] — 此功能用来验证入站邮件中的域名密钥标识邮件 (DKIM)。当一封入站邮件已加密签名，SecurityGateway 将从签名中取出域的 DNS 记录来检索公共密钥，然后使用该密钥来测试邮件的 DKIM 签名来决定其是否有效。若 DKIM 签名通过了验证测试，邮件将以常规的投递步骤继续下一步操作并且可随意调整其邮件总值[143]。DKIM 验证不仅能够保证一份邮件来自于假定的发件人，而且没有修改从签名时间到发送给您的时间。

DKIM 签名[155] - 这个签名选项用于控制您域的出站 邮件是否使用 DomainKeys Identified Mail (DKIM) 进行加密签名。您也可创建要用来给域邮件签名的选择器和密钥，并且指定将使用哪个选择器。

DMARC[158] - 提供以下三个部分供您配置 SecurityGateway 的 DMARC 验证和报告功能：DMARC 验证、DMARC 报告和 DMARC 设置。

回叫验证[169] — 回叫验证是一种反诈骗的方法，用来确认一封入站邮件的假定发件人的邮件地址是否有效。要执行此操作，SecurityGateway 将连接至在 SMTP 会话过程中通过 "邮件发件人"语句的域邮件交换器，并试图验证该发件人地址是不是此域中的有效地址。若检查的结果显示该发件人地址不存在，那么 SecurityGateway 将把其视为来自于一个伪造地址的邮件，因此会拒收该邮件，隔离它，或者接受它然后任意地调整它的 邮件总值[143] 并在主题上添加一个标记。

发件人报头屏蔽[171] - 该页面包含一些选项，有助于揭露垃圾邮件发送者发送的邮件中存在欺骗性的 "发件人"报头，这可能诱使用户相信邮件是从合法来源发送的。

4.3.1 反向查询

PTR

在入站 SMTP 连接上执行反向 PTR 记录查询
默认情况下，SecurityGateway 在所有的入站 SMTP 连接上执行 PTR 查询。如果您不希望这样做，请清除该选项。

如果不存在 PTR 记录 (警惕)，发送 501 并关闭连接
如果选中此框，当该域中不存在 PTR 记录时，SecurityGateway 将发送501错误代码 (参数中的句法错误)并关闭连接。默认情况下，禁用该选项。

如果没有 PTR 记录匹配，发送 501 并关闭连接
如果选中此框，PTR 记录查询结果无法匹配时，SecurityGateway 将发送501错误代码 (参数中的句法错误)并关闭连接。默认情况下，禁用该选项。

将已验证的会话从惩罚性操作中排除
当启用该复选框，SecurityGateway 会将入站 SMTP 连接上的 PTR 查询延迟至 SMTP MAIL 命令之后，以查看该连接是否使用验证。如果是经验证的会话，就不会对发件人采取惩罚性措施。默认情况下，禁用该选项。

将列于全局允许列表中的 IP 地址从惩罚性操作中排除
如果您希望将全局性地列于允许列表的 IP 地址[40]从 PTR 记录查询中排除，请单击该复选框。默认情况下，禁用该选项。

HELO/EHLO

在 HELO/EHLO 域上执行查询
默认情况下，SecurityGateway 会查询在会话的HELO/EHLO期间报告的域名。客户端（发送机）使用 "HELO/EHLO"命令来向服务器标识自己。在这项命令中服务器会使用由客户端通过的域名以填充 "已接收"报头中的 "发件人"部分。如果您不希望执行这些查询，请禁用该选项。

对伪造的标识发送 501 并关闭连接（警告）
如果您希望当查询结果表明是一个伪造的标识时发送 501 错误代码并关闭连接，请点击该复选框。默认情况下，禁用该选项。

> 当反向查询的结果表明服务器正在使用一个伪造的标识时，该结果可能经常不正确。邮件服务器使用不匹配其 IP 地址的值来标识自己很常见。这是由 ISP 限制与约束以及其他合法理由造成的。所以请慎用该选项。使用该选项可能会导致您的服务器拒收一些合法邮件。

如果查询返回 "未找到域"，则拒收邮件
当查询结果是 "未找到域"时，启用该选项会拒收邮件并发送 "451"错误代码（请求的操作中止：处理中发生本地错误）之后对话将照常进行。默认情况下，禁用该选项。

...发送 501 错误代码（通常发送 451 错误代码）
如果您希望出现 "域未找到"查询结果时发送 501 错误代码（参数中的句法错误）取代 451 错误代码，请启用该选项。

...然后关闭连接
如果您希望在反向查询的结果是 "未找到域"时立刻关闭连接而不是继续进行时，请点击该复选框。

将已验证的会话从惩罚性操作中排除
当启用该复选框，SecurityGateway 会将入站 SMTP 连接上的查询延迟至 SMTP MAIL 命令之后，以查看该连接是否使用验证。如果是经验证的会话，就不会对发件人采取惩罚性措施。默认情况下，禁用该选项。

将列于全局允许列表中的 IP 地址和主机从惩罚性操作中排除
如果您希望将全局性地列于允许列表的 IP 地址[40]与全局性地列于允许列表的主机[215]从 HELO/EHLO 域上的查询中排除，请单击该复选框。默认情况下，禁用该选项。

邮件

执行查询 MAIL 命令中通过的值
默认情况下，SecurityGateway 会查询在邮件传输的 MAIL 命令中通过的域名。"MAIL"命令中通过的地址应该是邮件的反向路径，并且该地址通常就是发送邮件的邮箱。但有时，

它也会是错误邮件应被指向的地址。如果您不希望在 MAIL 值上执行查询，请禁用该选项。

...对伪造的标识发送 501 并关闭连接 (警告)
如果您希望当查询结果表明是一个伪造的标识时发送 501 错误代码并关闭连接，请点击该复选框。默认情况下，禁用该选项。

当反向查询的结果表明服务器正在使用一个伪造的标识时，该结果可能经常不正确。邮件服务器使用不匹配其 IP 地址的值来标识自己很常见。这是由 ISP 限制与约束以及其他合法理由造成的。所以请慎用该选项。使用该选项可能会导致您的服务器拒收一些合法邮件。

如果查询返回“未找到域”，则拒收邮件
默认情况下，当 MAIL 值上的查询结果是 “域未找到”，将拒收邮件并发送451错误代码 (请求的操作中止：处理中发生本地错误)之后对话将照常进行。如果您不希望拒收这些邮件，请清除该复选框。

...发送 501 错误代码 (通常发送 451 错误代码)
如果您希望出现 “域未找到”查询结果时发送 501 错误代码 (参数中的句法错误) 取代 451 错误代码，请启用该选项。

...然后关闭连接
如果您希望在反向查询的结果是 “域未找到”时立刻关闭连接而不是继续进行时，请点击该复选框。

排除来自经身份验证会话的邮件
默认情况下，会将通过已验证的会话的邮件从 MAIL 命令值上的查询中排除。如果您不希望排除那些邮件，请禁用该选项。

排除列入全局允许列表的发件人
默认情况下，将任何来自全局性列于允许列表发件人的邮件从查询中排除。如果您不希望排除来自那些发件人的邮件，请清除该复选框。

配置

对可疑邮件插入警告报头
默认情况下，SecurityGateway 将对任何反向查询失败的邮件插入警告报头。接收邮件的服务器或客户端就可以选择性地使用该报头来过滤邮件。如果您不希望对可疑的邮件插入警告报头，请清除该框。

4.3.2 SPF 验证

发件人策略框架 (SPF)是一个开放标准用以识别邮件中伪造的发件人地址。它尤其保护 SMTP 信封发件人地址或返回路径中的域。它通过检查域中用于 SPF 策略的 DNS 记录以精确地查出哪台邮件主机可以代表域发送邮件，从而做到如上所述。如果域有 SPF 策略而发件主机并没有列于该策略下，那么您就可以知道该地址是伪造的。

要了解有关 SPF 的更多信息，请访问：www.open-spf.org

配置

使用 SPF 校验发件主机

默认情况下，SecurityGateway 将检查发送域的 DNS 记录以查看发件主机是否有权代表该域发送邮件。这会使用在 SMTP 处理中通过的 MAIL 值中的域。如果您不希望使用 SPF 处理，请清除该复选框。

当 SPF 处理返回 HARD FAIL 结果时：

当邮件的 SPF 处理结果为 HARD FAIL 时，会采取以下操作。

...拒收邮件

默认情况下，收到 HARD FAIL 的邮件将在 SMTP 进程中被拒收。

...隔离邮件

如果您希望隔离收到 HARD FAIL 的邮件，请选择该选项。

...接受邮件

如果您希望接收收到 HARD FAIL 的邮件，请选择该选项。您可以随后对邮件主题插入某些文本并修改其邮件总值。

...以 [文本] 标记主题

当您将 SecurityGateway 配置为接收收到 HARD FAIL 结果的邮件时，若您希望向邮件的主题报头开头添加某些文本，启用该选项并指定要加入的文本。若启用，添加到主题的默认文本是：“*** FRAUD ***”。使用该选项，你可以将邮件留给收件人的邮件服务器或客户端以根据此标签来过滤邮件。默认情况下，禁用该选项。

您可在 SecurityGateway 中的多个其他地方选择添加文本到主题报头。比如，DKIM 验证 154 与邮件总值 143 页面也有这选项。当指定文本在这些选项中与条件匹配，仅会将该标签添加至邮件主题一次，即使那封邮件在各个选项下满足了此条件。但是，如果选项间的文本不同，那么仍将添加每一个唯一的标签。比如，该选项的默认文本是“*** FRAUD ***”，而邮件总值中的默认文本是“*** SPAM ***”。因为两个标签不同，匹配这两个选项条件的邮件都会添加这两个标签。但是，如果您更改了其中一个选项内的文本，使之等同于另外一个文本，那么仅会添加该标签一次。

...添加 [xx] 点数到邮件总值

默认情况下，当你将 SecurityGateway 配置为接收收到 HARD FAIL 结果的邮件时，会将该值添加至其邮件总值。如果最终总值足够高，就会根据您的邮件评值 143 设置，隔离或拒收邮件。该选项的默认值是5.0。

当 SPF 处理返回 SOFT FAIL 结果时：

当 SPF 处理邮件的结果为 SOFT FAIL 时，会采取以下操作。

...拒收邮件

如果您希望在 SMTP 进程中拒收收到 SOFT FAIL 的邮件，请点击该选项。

...隔离邮件
如果您希望隔离收到 SOFT FAIL 的邮件，请选择该选项。

...接受邮件
默认情况下，会接收收到 SOFT FAIL 的邮件，但是您可以随后将某些文本插入至邮件主题并修改其邮件总值。

...以[文本]标记主题
当您将 SecurityGateway 配置为接收收到 SOFT FAIL 结果的邮件时，若您希望向邮件的主题报头开头添加某些文本，启用该选项并指定要加入的文本。若启用，添加到主题的默认文本是："*** FRAUD ***"。使用该选项，你可以将邮件留给收件人的邮件服务器或客户端以根据此标签来过滤邮件。默认情况下，禁用该选项。

...添加 [xx] 点数到邮件总值
默认情况下，当你将 SecurityGateway 配置为接收收到 SOFT FAIL 结果的邮件时，会将该值添加至其邮件总值。如果最终总值足够高，就会根据您的邮件评值 143 设置，隔离或拒收邮件。该选项的默认值是2.0。

当 SPF 处理返回 PASS 结果时：

...添加 [xx] 点数到邮件总值
如果您希望邮件的 SPF 处理结果是 PASS 时调整邮件总值，请点击该选项。这应该为一个负数，以减少邮件总值，从而进行有利的调整。

例外

排除来自被列入允许列表的 IP 地址的邮件
如果您希望在发件人的 IP 地址出现在全局 IP 允许列表 217 时，将该发件人从 SPF 处理中排除，请点击该复选框。默认情况下，禁用该选项。

排除来自经身份验证会话的邮件
默认情况下，如果接收的邮件正在使用已认证的会话，会将其从 SPF 处理要求中排除。如果您希望在 SMTP 会话通过验证时，仍旧使用 SPF 处理，请清除该选项。

排除来自域邮件服务器的邮件
默认情况下，发送自您域邮件服务器 66 的邮件将从 SPF 处理中免除。如果您不希望将域邮件服务器从 SPF 要求中免除，请清除该复选框。

高级

插入 "Received-SPF" 报头到邮件中
默认情况下，"Received-SPF" 报头会插入到每封邮件中，包括用于邮件的 SPF 结果。如果您不希望插入该报头，请清除该复选框。

……除非 SPF 结果为 "none"
默认情况下，当 SPF 查询结果为 "none" 时，不会插入 "Received-SPF" 报头。如果您希望在发件人的域中没有发现 SPF 数据的情况下仍然插入报头，请不要勾选该选项。

例外 - 域

当配置这些设置时，如果您在页面顶部的 *"针对域："* 下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。在相应的域中点击 *"查看/编辑"* 链接以查看或者编辑其 SPF 设置，或点击 *"重置"* 以将域的设置重置回默认的全局值。

4.3.3 DKIM 验证

使用此页面来配置 SecurityGateway，使其验证入站邮件中的域名密钥标识邮件 (DKIM)以及域名密钥 (DK)签名。当此项功能已启用且一封入站邮件已加密签名[155]时，SecurityGateway 将从签名中取出域的 DNS 记录来检索公共密钥，然后使用该密钥来测试邮件的 DKIM 签名来决定其是否有效。若 DKIM 签名通过了验证测试，邮件将以常规的投递步骤继续下一步操作并且可随意调整其邮件总值[143]。

有关于 DKIM 的更多信息，请参阅：www.dkim.org。

加密校验

验证使用域名密钥标识邮件 (DKIM)而创建的签名
根据默认，SecurityGateway 将验证使用 DKIM 签名[155]的邮件。若您不希望验证邮件中的 DKIM 签名，那么请清理此选择框。

当验证返回 PASS 结果：

...添加 [xx]点数到邮件总值
当邮件从 DKIM 验证处收到 "通过"结果时，若您希望调整邮件分数，请使用此选项。根据默认，此选项的值设为 0.0，表示不会出现分值调整。如果您选择了调整这些邮件的分值，您应该在此选项中使用一个负值，这样便为邮件分数做出了有益的调整。例如，在此选项中使用 -0.5 将使最终分值降低 0.5。

例外

排除来自被列入允许列表的 IP 地址的邮件
根据默认，来自于已列入允许列表的 IP 地址[217]的邮件将无需受到 DKIM 验证。即使发件人已在 IP 地址允许列表中，您还是希望验证 DKIM 签名，请清除此选择框。

排除来自经身份验证会话的邮件
根据默认，来自于已验证 SMTP 会话的邮件无需受到 DKIM 验证。即使 SMTP 会话已通过验证，您还是希望验证 DKIM 签名，请清除此选择框。

排除来自域邮件服务器的邮件
根据默认，来自于您其中一个域邮件服务器[66]的邮件无需受到 DKIM 验证。如果您希望验证来自于域邮件服务器邮件的 DKIM 签名，请清除此选择框。

DKIM 验证选项 (所有域)

验证程序接受正文长度计数 ("l="标记)
启用该选项后，SecurityGateway 将会接受在入站邮件的 DKIM 签名中所找到的正文长度计数标记。若真实的正文长度计数大于该标记中所包含的值，SecurityGateway 将只验证标记中指定的数量，邮件的余下部分将不验证。这就表明邮件中有附加内容，因而不验证的部分可认为是可疑的。若真实的正文长度小于该标签中所包含的值，该签名将不

会通过验证（例如：它将收到一个“失败”结果）。这就表明，邮件中的一些部分已被删除，从而导致正文长度计数不足该标记中所指定的数量。默认情况下，禁用该选项。

验证程序需要签名来保护“主题”报头
若您需要入站邮件的 DKIM 签名来保护主题报头，请启用此选项。默认情况下，禁用该选项。

例外 - 域

当配置这些设置时，如果您在页面顶部的*“针对域：”*下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。点击 *查看/编辑* 相应域的链接来查看或编辑其 DKIM 验证设置，或者点击*重置*，将域设置重置为默认的全局值。

4.3.4 DKIM 签名

使用“DKIM 签名”页面上的选项可以控制是否使用 DomainKeys Identified Mail (DKIM) 对域的出站邮件进行加密签名。您也可使用该页面来创建用于签名域邮件的选择器和密钥，并且指定将使用哪个选择器。每一个的密钥都是唯一的——两个域不可能存在相同的密钥，无论选择器指定与否。

有关于 DKIM 的更多信息，请参阅：www.dkim.org。

DKIM 签名

使用域名密钥标识邮件 (DKIM) 来签名出站邮件
如果您希望使用域名密钥标识邮件来加密性签名域的出站邮件，请点击此选项。要签名一封邮件，必须由 SecurityGateway 通过 SMTP AUTH 在已验证的会话上接收，或从域邮件服务器 66 进行接收。这是为了在签名之前确保邮件是真实的。

ARC 签名

ARC 是一种电子邮件身份验证协议，当 SecurityGateway 作为邮件的中间服务器时，它允许对入站邮件的身份验证结果进行数字签名，以便当邮件继续到达最终目的地时，它仍然可以通过接收方的服务器进行验证。例如，当 SecurityGateway 重定向邮件或处理需要修改邮件 DKIM 签名中包含报头的邮件列表邮件时，这很有用。当收件服务器使用 ARC 验证 162，并将您的 SecurityGateway 域指定为可信 ARC 封签者 162，它便能验证您的 ARC 签名并将邮件作为真实邮件接收。

使用 ARC 签名合法邮件
如果您希望使用 ARC 来签名合法邮件，请选中此框。来自本地域的邮件无需 ARC 签名，因为它们可以进行 DKIM 签名。因此，所有不是来自本地域的出站邮件都有资格进行 ARC 签名。当 SecurityGateway 修改邮件或 DKIM 签名中包含的任何邮件报头时，ARC 签名是必要的。这些修改可能包含以下操作，例如发件人报头屏蔽 171、添加免责声明 95 或更小的变更。请注意，启用 ARC 签名后，将对并非源自本地域的所有出站邮件进行签名，而不仅仅是那些已修改的邮件。默认情况下禁用 ARC 签名。

有关 ARC 协议的更多信息，请参阅：RFC 8617: The Authenticated Received Chain (ARC) 协议.

选择器

使用此选择器来签名邮件：
从下拉列表中选择选择器，当签名域邮件时，该选择器的相应公钥/私钥对是您想要使用的。如果您希望创建一个新选择器，点击 *"新建"*按钮，在给出的空间内键入想要的 *"选择器名称"*，然后点击 *"保存并关闭"*。

新建
点击此按钮来创建用于签名域邮件的新选择器。在给出的空间内输入选择器的名称然后点击保存并关闭。

导入
如果您希望导入 RSA 公钥/私钥对，并创建一个新的选择器，请点击**导入**。它必须是 .zip 文件，并以 PEM 格式包含 rsa.private 和 rsa.public 文本文件。您必须为选择器及其关联域选择名称 (或将其设置为全局选择器)。

导出
选择一个选择器并点击**导出**来以 .zip 文件下载该选择的 RSA 公共/私人密钥对。

删除
要删除一个选择器，请从下拉清单框中选中然后点击 *"删除"*。

查看该选择器的 DNS 配置 (公钥)
从下方下拉清单框中选中一个选择器，然后点击此按钮来查看该选择器的 DNS 配置。这是必须置于域 DNS 记录中的 DKIM 信息。DNS 记录中若没有该信息，就无法验证您邮件的签名。DNS 配置页面上列出了以下信息：

DNS 的 DKIM 选择器记录
其他服务器上会用到该信息，用于验证域的 DKIM 已签名邮件。其中包含选择器、域、公钥以及其他必要的信息。

如果您希望签名域的出站邮件，就需要将该信息置于域的 DNS 记录中。倘若没有，收件服务器将无法验证此签名。要了解更多信息以及可能包含于 DNS 记录中的其他参数，请访问 www.dkim.org 以及 domainkeys.sourceforge.net 上的域名密钥分发选项页面。

使用共享/全局选择器

当您希望为多个 SecurityGateway 域使用同一选择器时，有两种方法可以执行此操作：

为每个域将单独的 DKIM 选择器记录发布到 DNS，但使用相同的公钥

1. 在 "针对域:" 选项，选择 "-- 全局 --"。
2. 选择一个选择器或创建一个新的选择器，然后点击**查看此选择器的 DNS 配置 (公钥)**。
3. 复制 **DNS 的 DKIM 选择器记录** 下的文本。
4. 在 DNS 中，为将共享选择器的域之一创建 DKIM 选择器时粘贴该文本，但使用该域名替换 **%DOMAIN%**。例如，替换 "selector01._domainkey.%DOMAIN%." 的是 "selector01._domainkey.example.com."。

5. 对将共享选择器的每个域重复这些步骤。
6. 请确保为所有相关域正确配置了 DKIM 签名选项，以便使用共享选择器进行签名。

将 DKIM 选择器记录发布到一个域的 DNS，然后使用 CNAME 将其他域指向该域

1. 选择一个选择器，并使用 "查看此选择器的 DNS 配置（公钥）"下的文本来发布 DNS 中的 DKIM 记录，用于您的一个域。例如：

```
selector01._domainkey.example.com IN TXT "v=DKIM1;
  p=MIGfMA0GCSq..."
```

2. 对于将共享选项器的每个域，请为 "selector01._domainkey"子域设置一个 CNAME 记录来指向原始域。例如：

   example01.com - `selector01._domainkey.example01.com IN CNAME selector01._domainkey.example.com`

   example02.com - `selector01._domainkey.example02.com IN CNAME selector01._domainkey.example.com`

3. 请确保为所有相关域正确配置了 DKIM 签名选项，以便使用共享选择器进行签名。

DKIM 签名选项（所有域）

签名在 [xx]天后到期（"x="标签，默认为七天）
使用此选项来限制 DKIM 签名的有效天数。如果邮件的签名已到期，那么该邮件将总无法通过验证。该选项对应的是签名的 "x="标签。根据默认已经启用且设置为七天。

签名包括查询方式（包括 "q="标签）
该选项用于在 DKIM 签名中包含查询方式标签（例如：q=dns）。根据默认已包含其中。

签名包括正文长度计数（包括 "l="标签）
该选项控制了在 DKIM 签名中是否要包括正文长度计数（"l="标签）。默认情况下启用此项。

签名包括原始报头内容（包括 "z="标签）
如果您希望在 DKIM 签名中包含 "z="标签，请点击此选项。该标签将包含邮件原始报头的副本，从而可以使签名变得非常大。默认情况下，禁用该选项。

规范化

规范化是一个将邮件的报头和正文转化为规范化的标准，并在创建 DKIM 签名之前将其 "常规化"的过程。这样做是必要的，因为在常规处理的过程中，一切邮件服务器和中继系统会对邮件做出各种无关紧要的改变，如若在准备签名每封邮件时不使用规范化的标准，那么可能会造成签名被破坏。目前有两种用于 DKIM 签名和验证的规范化方法：简单和轻松。简单是最严谨的方法，不允许对邮件做出改变，或只允许细微改变。轻松则要求相对较送，允许一些无关紧要的改变。

规范化报头使用：简单，轻松
这是在签名邮件时用于邮件报头的规范化方法。简单表示在任何情况下都不允许对报头字段进行更改。轻松则允许将报头名称转换为小写（不是改变报头的值），将一个或多个连续空格转换为一个空格，以及其他一些无害改变。默认设置为"简单"。

规范化正文使用：简单，轻松
这是在签名邮件时用于邮件正文的规范化方法。简单可忽略邮件正文末尾的空行——不再允许其他任何对于邮件正文的更改。轻松则允许邮件末尾的空白行，忽略行末尾的空格，将一行中的所有连续空格减少为一个空格字符，以及其他一些小的更改。默认设置为"简单"。

4.3.5 DMARC

基于域的邮件验证、报告和一致性（DMARC）这个规范旨在减少邮件滥用（例如通过伪造邮件的"From:"报头。）DMARC 帮助域拥有者使用"域名系统"（DNS）来向收件服务器告知其 DMARC 策略，例如他们希望这些服务器如何处理自称来自他们域但无法验证实际来源的邮件。收件服务器在处理入站邮件时通过 DNS 查询检索到的这个策略，可以向服务器表明应该隔离或拒收不符合这个策略的邮件，或根本不采取任何操作（例如继续照常处理邮件）。除了这个策略以外，该域的 DMARC DNS 记录也可以包含服务器请求来向某人发送 DMARC 报告、概述自称来自此域的入站邮件的总数、它们是否通过验证、以及任何失败的详细信息。DMARC 的报告功能在确定您的邮件验证流程是否有效，以及伪造邮件使用您域名的频率时极其有用。

在"**安全 » 反欺诈**"下，提供以下三个部分供您配置 MDaemon 的 DMARC 验证和报告功能：DMARC 验证、DMARC 报告和 DMARC 设置。

DMARC 验证 162

作为 DMARC 验证流程的一部分，SecurityGateway 对在每封入站邮件的"From:"报头中找到的域执行 DMARC DNS 查询。这用来确定该域是否使用 DMARC，如果使用了 DMARC 则检索其"DMARC DNS 记录 159"，其中包含了它的策略和其他 DMARC 相关信息。此外，DMARC 使用 SPF 151 和 DKIM 154 来验证每封邮件，并要求它至少通过一项测试来通过 DMARC 验证。如果该邮件通过验证，则按照 SecurityGateway 其余投递和过滤流程来照常处理这封邮件。如果未通过验证，则取决于该域的 DMARC 策略以及您对于 SecurityGateway 如何处理这些邮件的配置来确定该邮件的命运。

如果一封邮件未通过 DMARC 验证，而且 DMARC 域拥有一个"p=none"策略，则不会采取任何惩罚性操作并照常处理这封邮件。当 DMARC 域拥有"p=quarantine"或"p=reject"限制策略时，SecurityGateway 可以有选择性地将该邮件自动过滤到接收用户的隔离文件夹 255，向其主题报头添加一些文本或调整其邮件分值 143。对于使用限制性策略且未通过验证的邮件，SecurityGateway 将取决于策略插入"X-SGDMARC-Fail-policy: quarantine"或"X-SGDMARC-Fail-policy: reject"报头。这帮助您使用 Sieve 脚本 219 或您邮件服务器的内容过滤器系统来基于这些报头来执行一些操作，例如将该邮件发送至特定的文件夹进行审核。

建议默认情况下为大多数 SecurityGateway 配置启用 DMARC 验证。

DMARC 报告 165

在 SecurityGateway 查询 DNS 是否存在 DMARC 记录时，该记录可能包含一些标签，指示域的拥有者是希望接收与声称来自此域邮件相关的 DMARC 综合报告还是故障报告。"DMARC 报告"屏幕上的一些选项供您用来指定是否希望发送请求的报告类型，并指定

这些报告应该包含的元数据。将在每晚午夜 (UTC)发送综合报告，将按邮件来发送故障报告，因为每个发生的事件将触发这个报告。报告以打包压缩 (ZIP)的 XML 文件附件形式发送，而且在线提供各种分析工具，帮助收件人更简便地进行查看。默认情况下，SecurityGateway 仅发送汇总报告。

DMARC 设置

"DMARC 设置"屏幕包含各种选项，例如在 DMARC 报告中包含特定信息、记录 DMARC DNS 记录、以及更新 SecurityGateway 用于 DMARC 的 "公共后缀"文件。

DMARC 验证和邮件列表

因为 DMARC 的目的在于确保在邮件 "From:"报头中找到的域不被伪造，必须允许发件服务器代表该域来发送邮件。这会给邮件列表带来一个问题，因为列表通常代表来自外部域的列表成员来分发邮件，并使 "From:"报头保持不变。这就意味着在收件服务器尝试对这些邮件使用 DMARC 验证时，邮件会被不关联 "From:"报头域的服务器发送。如果 DMARC 域正好使用了存在限制的 DMARC 策略，这会导致邮件被隔离甚至被收件服务器拒收。在某些情况下，这会导致从列表的成员中删除收件人。为了规避这个问题，你应该配置域名邮件服务器来使用邮件列表地址替换 "发件人:"报头中的发件人地址，或者将它们配置为在来自具有限制性 DMARC 策略的域时拒绝接受列表中的任何邮件。如果您的邮件服务器时 MDaemon 14.5 或更高版本，默认情况下在发件人的域使用限制性 DMARC 策略时，它将使用邮件列表地址来替换 "发件人:"报头。

为您的域使用 DMARC

如果您希望为您自己的域使用 DMARC，这就意味着您希望支持 DMARC 的收件服务器使用 DMARC 来验证声称由您发送的邮件，您首先必须确保您已为该域创建了格式正确的 SPF 和 DKIM DNS 记录；而且您必须使这些选项正确工作来使用 DMARC。如果您正在使用 DKIM，您也要配置 SecurityGateway 的 "DKIM 签名"选项来签署该域的邮件。此外，您必须为该域创建一个 DMARC DNS 记录。通过查询 DNS 是否存在这个拥有特殊格式的 TXT 记录，收件服务器可以确定您的 DMARC 策略和各种可选的参数，例如：您使用的验证模式、您是否希望接收综合报告、应接收报告的邮件地址等。一旦您正确配置了 DMARC 并开始接收 DMARC XML 报告，您可以使用大量在线工具来阅读这些报告并诊断任何潜在的问题。

定义 DMARC TXT 资源记录

以下是 DMARC 记录常用组件的基本概述。要获得更多详细信息或有关高级配置的更多信息，请参阅：www.dmarc.org。

拥有者字段

DMARC 资源记录的 "拥有者"(也叫做 "姓名"或 "左侧")字段必须始终为 **_dmarc**，如果您希望指定该记录应用到的域或子域，也可以采用 **_dmarc.domain.name** 这种形式。

示例：

域 **example.com** 的 DMARC 记录

```
_dmarc IN TXT "v=DMARC1;p=none"
```

该记录将应用于发自 user@example.com 或子域为 example.com 的电子邮件，例如 user@support.example.com、user@mailsupport.example.com 等。

```
_dmarc.support.example.com IN TXT "v=DMARC1;p=none"
```
该记录仅应用于发自 user@support.example.com 的电子邮件，不应用于发自 user@example.com 的电子邮件。

```
_dmarc.support IN TXT "v=DMARC1;p=none"
```
该记录将应用于发自：user@support.example.com、user@a.support.example.com、user@a.b.support.example.com 等的电子邮件。

DMARC 记录标签和值

必需标签

标签	值	便笺
v=	**DMARC1**	这是“版本”标签，必须作为该记录的 DMARC 特定文本部分的第一个标签。即使其他 DMARC 标签值不区分字母大小写，**v=** 标签的值必须是大写字母：**DMARC1**。 示例： `_dmarc IN TXT "v=DMARC1;p=none"`
p=	**none** **quarantine** **reject**	这是“策略”标签，必须作为 DMARC 记录中的第二个标签，紧接 **v=** 这个标签。 **p=none** 表示收件服务器基于 DMARC 查询结果不采取任何操作。不得基于未通过 DMARC 检查这个失败隔离或拒收邮件。不过可以出于其他理由隔离或拒收这些邮件，例如未通过垃圾邮件过滤测试或与 DMARC 无关的其他安全检查。对于 **p=none** 的使用有时被称为“监控”或“监控模式”，因为您可以配合 **rua=** 这个标签一起使用来从收件域接收有关您邮件的综合报告，不过不会对未通过 DMARC 检查的这些邮件执行任何惩罚性操作。您可以一直使用这个策略，直到您彻底测试了您的 DMARC 实施，并确保您已准备好使用更具有限制性的 **p=quarantine** 策略。 **p=quarantine** 这个策略用于以下场景：在邮件的 **“From:”** 报头声称由您所发送但未通过 DMARC 检查时，您希望其他邮件服务器将该邮件视为可疑邮件。取决于服务器的本地策略，这可以表示对邮件进行额外审核、将其放入收件人的垃圾邮件文件夹、将其路由到不同的服务器或采取其他操作。 **p=reject** 表示您希望收件服务器拒收未通过 DMARC 验证的任何邮件。不过一些服务器仍然接收这些邮件，不过将其隔离或进行额外审核。这是限制性最高的策略，通常不使用该策略，除非您对自己的邮件策略、以及您允许账户使用的邮件或服务类型把握十足。例如，如果您允许您的用户加入第三方邮件列表，使用邮件转发服务，并使用网站上的“共享”功能，使用 **p=reject** 将可能导致一些合法邮件被拒收。而且该设置也会使某些用户被一些邮件列表删除或阻止。 示例：

		`_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:dmarc-report@example.net"`

额外标签

以下列出的所有标签都是可选标签。如果未在记录中使用任何这些标签，则假定其默认值。

标签	值	便笺
sp=	**none** **quarantine** **reject** — 默认值： 如果未使用 **sp=**，则对域和子域应用 **p=** 这个标签。	此标签用来指定应用 DMAR 记录的域的子域将使用的策略。例如，如果应用于 example.com 的记录中使用了这个标签，那么会将 **p=** 这个标签中指定的策略应用于来自 example.com 的邮件，将 **sp=** 这个标签中指定的策略应用于来自 example.com 子域的邮件，例如 mail.example.com。如果在记录中忽略了这个标签，则将 **p=** 这个标签应用于该域及其子域。 示例： `_dmarc IN TXT "v=DMARC1;p=quarantine;sp=reject"`

rua=	由逗号分隔的将接收 DMARC 综合报告的邮件地址列表 必须使用以下格式输入作为 URI 的 地址：**mailto:user@example.com**
	—
	默认值：**none**
	如果未使用这个标签，则不发送综合报告。
		此标签表示您希望从接收了一封 **From:**”声称来自您所在域邮件的收件服务器接收 DMARC 综合报告。使用以下格式指定作为 URI 的一个或多个邮件地址：**mailto:user@example.com**，使用逗号分隔多个 URI。
		示例：
		`_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:user01@example.com,mailto:user02@example.com"`
		通常这些地址将位于此记录覆盖的域。如果您希望将报告发送至其他域的地址，则该域的 DNS 区域文件必须也包含一个专用的 DMARC 记录，指示它将接收该域的 DMARC 报告。
		example.com 的记录示例：
		`_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:non-local-user@example.net"`
		example.net 的记录：
		`example.com._report._dmarc TXT "v=DMARC1"`

ruf=	由逗号分隔的将接收 DMARC 故障报告的邮件地址列表 必须使用以下格式输入作为 URI 的 地址：**mailto:user@example.com**
	—
	默认值：none
	如果未使用这个标签，则不发送故障报告。
		此标签表示您希望从接收了一封 **From:**”声称来自您所在域邮件的服务器接收 DMARC 故障报告，前提是满足了在 **fo=** 这个标签中指定的条件。在默认情况下，如果未指定 **fo=** 这个标签，在邮件未通过所有 DMARC 验证检查时将发送故障报告 例如未通过 SPF 和 DKIM 验证）。使用以下格式指定作为 URI 的一个或多个邮件地址：**mailto:user@example.com**，使用逗号分隔多个 URI。
		示例：
		`_dmarc IN TXT "v=DMARC1;p=quarantine;ruf=mailto:dmarc-failures@example.com"`
		通常这些地址将位于此记录覆盖的域。如果您希望将报告发送至其他域的地址，则该域的 DNS 区域文件必须也包含一个专用的 DMARC 记录，指示它将接收该域的 DMARC 报告。
		example.com 的记录示例：
		`_dmarc IN TXT "v=DMARC1;p=quarantine;ruf=mailto:non-local-user@example.net"`
		example.net 的记录：
		`example.com._report._dmarc TXT "v=DMARC1"`

要了解有关 DMARC 规范的更多扩展信息，请参阅：www.dmarc.org。

4.3.5.1 DMARC 验证

作为 DMARC 验证流程的一部分，SecurityGateway 对在每封入站邮件的 “From:”报头中找到的域执行 DMARC DNS 查询。这用来确定该域是否使用 DMARC，如果使用了 DMARC 则检索其 “DMARC DNS 记录”，其中包含了它的策略和其他 DMARC 相关信息。此外，DMARC 使用 SPF 和 DKIM 来验证每封邮件，并要求它至少通过一项测试来通过 DMARC 验证。如果该邮件通过验证，则按照 SecurityGateway 其余投递和过滤流程来照常处理这封邮件。如果未通过验证，则取决于该域的 DMARC 策略以及您对于 SecurityGateway 如何处理这些邮件的配置来确定该邮件的命运。

如果一封邮件未通过 DMARC 验证，而且 DMARC 域拥有一个 “p=none”策略，则不会采取任何惩罚性操作并照常处理这封邮件。当 DMARC 域拥有 “p=quarantine”或 “p=reject”限制策略时，SecurityGateway 可以有选择性地将该邮件自动过滤到接收用户的隔离文件夹，向其主题报头添加一些文本或调整其邮件分值。对于使用限制性策略且未通过验证的邮件，SecurityGateway 将取决于策略插入 “X-SGDMARC-Fail-policy: quarantine”或 “X-SGDMARC-Fail-policy: reject”报头。这帮助您使用 Sieve 脚本或您邮件服务器的内容过滤器系统来基于这些报头来执行一些操作，例如将该邮件发送至特定的文件夹进行审核。

DMARC 验证

启用 DMARC 验证和报告
启用此项时，SecurityGateway 将对在入站邮件的 "From:" 报头中找到的域执行 DMARC DNS 查询，并按照您在 "DMARC 报告[165]"屏幕上所设置的发送综合和故障报告。DMARC 使用 SPF[151] 和 DKIM[154] 来验证邮件，因此必须至少启用其中一个功能才能使用 DMARC。默认情况下启用 DMARC 验证和报告，而且应用于大多数 SecurityGateway 配置。

启用 ARC 验证
勾选此框来启用 ARC 验证。ARC 是一种电子邮件身份验证协议，允许中间邮件服务器对邮件的身份验证结果进行数字签名，以便当邮件继续到达最终目的地时，即使 SPF 或 DKIM 验证可能因重定向或邮件列表修改而失败，它仍然可以进行验证。ARC 验证允许您指定您信任其 ARC 结果的域，以便通过查看这些结果，SecurityGateway 可以确定是否接受邮件。有关 ARC 协议的更多信息，请参阅：RFC 8617: The Authenticated Received Chain (ARC) 协议.

管理可信 ARC 封签者
点击此按钮可管理受信任的 ARC 封签者，这是您信任其 ARC 结果的域。在进行 DMARC 验证时，将忽略来自不可信域的 ARC 结果。

禁用 DMARC 支持会导致您的用户收到呈增长趋势的垃圾邮件、网络钓鱼邮件或其他伪造的邮件。在某些情况下还会引起您邮件服务器的一些邮件列表邮件被其他服务器拒收，甚至从您的列表中删除一些列表成员。您不得禁用 DMARC，除非您确认您必须那么做。

当验证返回 "REJECT" 结果时：
这是当入站邮件未通过 DMARC 验证过程，并且声称发送域的 DMARC DNS 记录设置为 p=reject 时将采取的操作。

...拒收邮件
如果您希望在 DMARC 验证过程返回 REJECT 结果时拒绝 SMTP 过程中的邮件，请使用此选项。默认情况下，选中该选项。

即使您选择不拒绝这些邮件，也可能因为某些其他原因（例如您的 SPF 或 DKIM 设置）或邮件分数高于允许的阈值而拒绝邮件。

...隔离邮件
当 DMARC 验证过程返回 REJECT 结果，如果您希望隔离[255]邮件而不是拒收，请选择此项。配合该选项，您还可以使用下方的 *"..使用 [text] 标记主题"* 和 *"..添加 [xx] 点到邮件分值"* 这两个选项。

...接受邮件
当选择此选项时，SecurityGateway 将接受从 DMARC 验证过程收到 REJECT 结果的邮件，但仍可以使用下方的选项来标记其主题报头并调整其邮件分值[143]。

...以 [文本] 标记主题
如果您已将 SecurityGateway 配置为接受或隔离无法通过 REJECT 指令进行 DMARC 验证的邮件，则启用此选项并指定一些文本（如果您希望将某些内容添加到邮件主题报头的开头）。若启用，添加到主题的默认文本是："*** FRAUD ***"。通过使用这个选项，您可以将邮件留给收件人邮件服务器或客户端，让他们根据标记来过滤邮件。默认情况下，该选项处于禁用状态。

您可在 SecurityGateway 中的多个其他地方选择添加文本到主题报头。例如，SPF 151 和邮件分数 143 页面均有此选项。当指定文本在这些选项中与条件匹配，仅会将该标签添加至邮件主题一次，即使那封邮件在各个选项下满足了此条件。但是，如果选项间的文本不同，那么仍将添加每一个唯一的标签。比如，该选项的默认文本是 "*** FRAUD ***"，而邮件总值中的默认文本是 "*** SPAM ***"。因为两个标签不同，匹配这两个选项条件的邮件都会添加这两个标签。但是，如果您更改了其中一个选项内的文本，使之等同于另外一个文本，那么仅会添加该标签一次。

...添加 [xx] 点数到邮件总值
默认情况下，当您将 SecurityGateway 配置成为具有 REJECT 策略指令的域接受或隔离 DMARC 验证失败的邮件时，此选项会将指定的值添加到邮件分值 143。如果最终分值足够高，就会根据您的 "邮件分值" 设置，隔离或拒收邮件。默认情况下，此选项将 5.0 点添加到 "邮件分值"。

当验证返回 QUARANTINE 结果时：
这是当入站邮件未通过 DMARC 验证过程，并且声称发送域的 DMARC DNS 记录设置为 p=quarantine 时将采取的操作。

...拒收邮件
如果您希望在 DMARC 验证过程返回 QUARANTINE 结果时拒绝 SMTP 过程中的邮件，请使用此选项。

...隔离邮件
当 DMARC 验证过程返回 QUARANTINE 结果，如果您希望隔离 255 邮件而不是拒收，请选择此项。配合该选项，您还可以使用下方的 *"..使用 [text] 标记主题"* 和 *"..添加 [xx] 点到邮件分值"* 这两个选项。默认情况下，选中该选项。

...接受邮件
当选择此选项时，SecurityGateway 将接受从 DMARC 验证过程收到 QUARANTINE 结果的邮件，但仍可以使用下方的选项来标记其主题报头并调整其邮件分值 143。

...以 [文本] 标记主题
如果您已将 SecurityGateway 配置为接受或隔离无法通过 QUARANTINE 指令进行 DMARC 验证的邮件，则启用此选项并指定一些文本（如果您希望将某些内容添加到邮件主题报头的开头）。若启用，添加到主题的默认文本是："*** FRAUD ***"。通过使用这个选项，您可以将邮件留给收件人邮件服务器或客户端，让他们根据标记来过滤邮件。默认情况下，该选项处于禁用状态。

您可在 SecurityGateway 中的多个其他地方选择添加文本到主题报头。例如，SPF[151] 和邮件分数[143]页面均有此选项。当指定文本在这些选项中与条件匹配，仅会将该标签添加至邮件主题一次，即使那封邮件在各个选项下满足了此条件。但是，如果选项间的文本不同，那么仍将添加每一个唯一的标签。比如，该选项的默认文本是 "*** FRAUD ***"，而邮件总值中的默认文本是 "*** SPAM ***"。因为两个标签不同，匹配这两个选项条件的邮件都会添加这两个标签。但是，如果您更改了其中一个选项内的文本，使之等同于另外一个文本，那么仅会添加该标签一次。

...添加 [xx] 点数到邮件总值
默认情况下，当您将 SecurityGateway 配置成为具有 QUARANTINE 策略指令的域接受或隔离 DMARC 验证失败的邮件时，此选项会将指定的值添加到邮件分值[143]。如果最终分值足够高，就会根据您的 "邮件分值"设置，隔离或拒收邮件。默认情况下，此选项将 2.0 点添加到 "邮件分值"。

例外

排除来自被列入允许列表的 IP 地址的邮件
根据默认，来自于已列入允许列表的 IP 地址[217]的邮件将无需受到 DMARC 验证。即使发件人已在 IP 地址允许列表中，您还是希望使用 DMARC 验证，请清除此选择框。

排除来自经身份验证会话的邮件
根据默认，来自于已验证 SMTP 会话的邮件无需受到 DMARC 验证。即使 SMTP 会话已通过验证，您还是希望使用 DMARC 验证，请清除此选择框。

排除来自域邮件服务器的邮件
根据默认，来自于您其中一个域邮件服务器[66]的邮件无需受到 DMARC 验证。若您希望使用来自于域邮件服务器邮件的 DMARC 验证，请清除此选择框。

4.3.5.2 DMARC 报告

在 SecurityGateway 查询 DNS 是否存在 DMARC 记录时，该记录可能包含一些标签，指示域的拥有者是希望接收与声称来自此域邮件相关的 DMARC 综合报告还是故障报告。"DMARC 报告"屏幕上的一些选项供您用来指定是否希望发送请求的报告类型，并指定这些报告应该包含的元数据。将在每晚午夜 (UTC) 发送综合报告，将按邮件来发送故障报告，因为每个发生的事件将触发这个报告。报告以打包压缩 (ZIP) 的 XML 文件附件形式发送，而且在线提供各种分析工具，帮助收件人更简便地进行查看。默认情况下，SecurityGateway 仅发送汇总报告。

只有启用了 "启用 DMARC 验证和报告"*这个选项位于* "DMARC 验证[162]"屏幕），该屏幕的选项才可用。此外，DMARC 规范要求使用报告收件人提供的 STARTTLS[100]。因此您应该尽可能启用 STARTTLS。

DMARC 报告

发送 DMARC 综合报告

如果您希望向要求 DMARC 综合报告的域发送该报告，请启用此项。如果对入站邮件的 "From:" 执行 DMARC DNS 查询时发现其 DMARC 记录包含 "rua=" 这个标签（例如 rua=mailto:dmarc-reports@example.com），这就表示该域的拥有者希望接收 DMARC 综合报告。因此 SecurityGateway 将存储有关此域和声称来自此域的入站邮件的 DMARC 相关信息。它会记录接收综合报告的邮件地址、每封邮件使用的验证方式（SPF、DKIM 或两者）、该邮件是否通过验证、发件服务器、其 IP 地址和应用的 DMARC 策略等。然后在每晚午夜（UTC），SecurityGateway 将使用存储的数据来生成各个域的报告，并将其发送至指定的地址。一旦发送了这些报告，已存储的 DMARC 数据将被清除，SecurityGateway 也将再次重新开始整个流程。

SecurityGateway 不支持对综合报告使用 DMARC 报告的间隔标签（例如 "i="）。SecurityGateway 从上次生成和发送 DMARC 报告后，在每晚午夜（UTC）将综合报告发送至为其编译了 DMARC 数据的任何域。

因为 SecurityGateway 必须在午夜 UTC 自动运行来发送综合报告并清除已存储的 DMARC 数据，如果您在那时关闭了 SecurityGateway，则不会生成任何报告，也不会清除 DMARC 数据。无论何时 SecurityGateway 再次运行，DMARC 数据收集都会继续，但不会生成报告，并且在下一次午夜 UTC 事件之前数据不会被清除。

发送 DMARC 故障报告（仅在发生事件时发送该报告）

如果您希望向要求 DMARC 故障报告的域发送该报告，请启用此项。如果对入站邮件的 "From:" 执行 DMARC DNS 查询时发现其 DMARC 记录包含 "ruf=" 这个标签（例如 ruf=mailto:dmarc-failure@example.com），这就表示该域的拥有者希望接收 DMARC 故障报告。这些报告不像综合报告那样是实时创建的，故障报告只在发生事件时才被触发，而且包含有关各个事件和故障错误的详细信息。域管理员可以使用这些报告来进行取证分析，并通过修改其邮件系统的配置来修复问题或识别其他问题，例如持续网络钓鱼攻击。

将触发故障报告的故障类型取决于该域的 DMARC 记录中 "fo=" 标签的值。默认情况下，仅在未通过所有基本的 DMARC 检查（例如未通过 SPF 和 DKIM）时才生成故障报告，不过域可以使用各种 "fo=" 标签值来表示它们希望仅在未通过 SPF、DKIM 或其他验证组合时就接收故障报告。因此，取决于在 DMARC 记录的 "ruf=" 标签中的收件人数量、"fo=" 标签的值、以及在邮件处理期间遇到的独立验证失败的数量，可以从一封邮件生成多个故障报告。如果您希望限制接收 SecurityGateway 将发送的指定报告的收件人数量，请使用下方的 *"准许至多这些 DMARC 'rua' 和 'ruf' 收件人"* 这个选项。

至于报告格式，SecurityGateway 只准许 "f=afrf" 这个标签（使用滥用报告格式的验证故障报告），这是 DMARC 的默认值。所有报告都以这个格式发送，即使域的 DMARC 记录含有 "f=iodef" 这个标签。

为了支持 DMARC 故障报告，SecurityGateway 完全支持：RFC 5965：邮件反馈报告的可扩展格式、RFC 6591：使用滥用报告格式的验证故障报告、RFC 6652：使用滥用报告格式的发件人策略框架 (SPF)验证故障报告、RFC 6651：针对故障报告的域名秘钥标识邮件 (DKIM)的扩展 和 RFC 6692：滥用报告格式 (ARF)报告中的源端口.

当 DMARC 的 "fo="标签要求报告 SPF 相关故障时，SecurityGateway 将按照 RFC 6522 来发送 SPF 故障报告。因此，在该域的 SPF 记录中必须存在那个规范的扩展。SPF 故障报告不独立于 DMARC 处理或在缺少 RFC 6522 扩展的情况下进行发送。

当 DMARC "fo="标签要求报告 DKIM 相关故障，SecurityGateway 将按照 RFC 6651 发送 DKIM 故障报告。因此，在 DKIM 签名报头字段中必须存在该规范的扩展，而且这个域必须在 DNS 中发布有效的 DKIM 报告 TXT 记录。DKIM 故障报告不独立于 DMARC 处理或在缺少 RFC 6651 扩展的情况下进行发送。

准许至多这些 DMARC "rua"和 "ruf"收件人 (0 = 无限制)
如果您希望限制将接收 SecurityGateway 所发送的指定 DMARC 综合报告或 DMARC 故障报告的收件人数量，请在此处指定最大值。如果 DMARC 记录的 "rua="或 "ruf="标签包含的地址数量大于您所指定的限制，那么 SecurityGateway 会将指定报告按顺序发送至列出的地址，直到达到地址最大值为止。默认情况下此限制被设置成 5。

将所有报告的副本通过电子邮件发送到：
在此处输入一个或多个由逗号分隔的电子邮件地址，来将所有 DMARC 汇总报告和 DMARC 失败报告的副本发送到这些地址 (仅 fo=0 或 fo=1)。

DMARC 报告元数据

使用这些选项来指定您公司或组织的元数据，会将这些数据包含于您所发送的 DMARC 报告中。

默认域
这是负责生成 DMARC 报告的 SecurityGateway 域。从下拉列表中选择域。

联系人邮件
使用此项来指定报告收件人在报告问题时可以联系的本地邮件地址。使用逗号来分隔多个地址。

联系信息
使用此项为报告收件人包含任何额外的联系信息，例如网站和电话号码等。

报告返回路径
这是用于 SecurityGateway 所发送的报告邮件的 SMTP 返回路径 (退回地址)，以防投递出现问题。使用 "noreply@<mydomain.com>"来忽略这些问题。

4.3.5.3DMARC 设置

"DMARC 设置"页面包含各种选项，例如在 DMARC 报告中包含特定信息、记录 DMARC DNS 记录、以及更新 SecurityGateway 用于 DMARC 的"公共后缀"文件。

DMARC 设置

在 DMARC 故障报告中包含 DKIM 规范化报头
如果您希望将 DKIM 规范化报头[155]包含于 DMARC 故障报告[165]中，则启用此项。默认情况下，禁用该选项。

在 DMARC 故障报告中包含 DKIM 规范化正文
如果您希望将 DKIM 规范化正文[155]包含于 DMARC 故障报告[165]中，则启用此项。默认情况下，禁用该选项。

前两个选项对调试问题很有用，不过在调试过程中不泄露任何邮件内容。

在 DMARC 报告中使用"X.X.X.X"替换保留的 IP
默认情况下，SecurityGateway 使用"X.X.X.X"替换您 DMARC 报告中的保留 IP 地址。如果您希望使您保留的 IP 在 DMARC 报告中可见，请禁用此项。此项不应用于 DKIM 规范化数据。

如果"发件人"与 DMARC 不兼容则拒收邮件
如果您希望在邮件的"发件人"报头结构与 DMARC 要求不兼容的情况下拒收这封邮件，请启用此项。这些是拥有多个"发件人"报头的邮件，或在一个"发件人"报头中拥有多个邮件地址的邮件。当前从 DMARC 处理中免除这些邮件。默认情况下禁用此设置，因为在一个"发件人"报头中拥有多个地址将在技术上引起协议违规，不过启用此设置有助于最大化 DMARC 保护。在启用 DMARC 验证[162]时仅应用这个设置。

插入"Precedence:bulk"报头到 DMARC 报告邮件
默认情况下 SecurityGateway 会将群发邮件报头插入 DMARC 报告邮件。如果您不希望插入该报头，请清除该复选框。

在日志文件中包含完整的 DMARC 记录
默认情况下 SecurityGateway 记录在 DMARC DNS 查询期间获得的完整 DMARC DNS 记录。如果您不希望在日志文件中包含完整的 DMARC 记录，请禁用此项。

如果公共后缀文件的存在时间大于这些天则进行自动更新
DMARC 需要公共后缀文件来确定查询 DMARC DNS 记录的正确域。默认情况下，每当 SecurityGateway 存储的公共后缀文件的存在时间大于 15 天，它将自动更新这些文件。如果您希望更新公共后缀文件的时间值大于或小于此值，请更改此项的值。如果您不希望进行自动更新，请禁用此项。

公共后缀文件 URL
这是 SecurityGateway 用来为 DMARC 下载公共后缀文件的 URL。默认情况下 SecurityGateway 使用位于以下位置的文件：
http://publicsuffix.org/list/effective_tld_names.dat。

立即更新公共后缀文件
点击此按钮来从上方指定的 *"公共后缀文件 URL"*手动更新公共后缀文件。

4.3.6 回呼验证

"回呼验证"是一种反诈骗的方法，用来确认一封入站邮件的假定发件人的邮件地址是否有效。要执行此操作，SecurityGateway 将连接至在 SMTP 会话过程中通过 "邮件发件人"语句的域邮件交换器，并试图验证该发件人地址是不是此域中的有效地址。如果检查的结果显示该发件人地址不存在，那么 SecurityGateway 将把其视为来自于一个伪造地址的邮件，因此会拒收该邮件，隔离它，或者接受它然后任意地调整它的邮件总值 143 或在主题上添加一个标记。一般而言，总有一些潜在问题和障碍与回呼验证相关联，所以根据默认该功能是禁用的。

要了解回呼验证的大致信息，请见 Wikipedia.org 上的 回呼验证文章。

配置

使用回呼验证来验证发件人
如果您想要使用回呼验证来检查发件人邮件地址有效与否，请点击此选择框。SecurityGateway 将会使用的值就是发件服务器在 SMTP 会话过程所通过的 "MAIL From"语句所通过的值，从而与假定发件人的域相连，然后验证此地址是否存在。根据默认，回呼验证已禁用。

首先尝试下验证命令（如果发件邮件服务器支持的话）
根据默认，当服务器指明其支持此验证命令时，SecurityGateway 首先会使用 SMTP "验证"命令来验证发件人的地址。服务器在 SMTP 会话刚开始时，通过向 SecurityGateway 回应 "250-VRFY"语句，以表明其支持验证命令。如果您要禁用此选项或者如果服务器不支持验证，那么 SecurityGateway 将使用 "MAIL From"以及"RCPT To"命令。SecurityGateway 验证域中发件人的地址是否有效，就是通过使用这些命令。看似准备发送邮件至一个有疑问的地址，不过其实没有发送任何邮件。

从该地址发送邮件：
当服务器不允许地址中的 NULL，或者当您禁用了下方的 *"先尝试地址中的 NULL"选项，那么在 "MAIL From"* SMTP 语句中，将适用此发件人地址。该选项的默认值是 "邮件管理员"。域部分将要附加的是收件人的域（例如：postmaster@RecipientsDomain.com）。如果您在此选项中指定一个完整的邮件地址，那么将以此地址来取代。举例来说，在此选项中使用 "xyz@example.com"就意味着将不再使用收件人的域。

没有一封真正地发送至了发件人邮件服务器。SecurityGateway 连接至服务器，并且发送 MAIL From 以及 RCPT To 命令，看似是准备发送一封邮件，但其实在还未发送任何邮件时便已终止连接。通过测试来查看服务器是否会接受一封发件人地址有疑问的邮件，SecurityGateway 就可以确认服务器认为该地址是否有效。

首先尝试 NULL 源地址
使用 "MAIL From"和 "RCPT To"命令来验证一个发件人地址时，SecurityGateway 会首先尝试使用一个带有 NULL 值的发件人 (例如："MAIL From <>")。如果该选项已被禁用或者服务器不允许 NULL 源地址，那么 SecurityGateway 会使用 *"从该地址发送邮件:"* 在此指定值。

如果发件人未通过回呼验证
如果回呼验证测试标明发件人的地址为无效，那么该邮件将被拒收、隔离、或接受下来，贴上可选的标签，并调整其邮件总值 143。对于未通过回呼验证的邮件，请在下列选项中选出您所希望的处理方式。

...拒收邮件
如果选择了此选项，那么在 SMTP 会话过程中，将会拒收未通过回呼验证的发件人的邮件。

...隔离邮件
如果您希望隔离未通过回呼验证的邮件，请选择此选项。这是默认选项。

...接受邮件
如果您希望接受未通过回呼验证的邮件，但希望调整其邮件分数或者在主题上添加一些文字，请使用此选项。

...以 [文本]标记主题
当发件人的邮件地址未通过回呼验证测试，如果您希望在邮件的主题报头上加一些内容，可点击该选项并指定一些文字。根据默认该选项是禁用的。若将其开启，根据默认 "*** CBV ***"将加入主题，不过如果您可选择对其进行编辑。

SecurityGateway 内还有一些其他位置，供您可以有选择性地将文本添加到 "主题"报头。例如，邮件分数 143和 URI 阻止列表 (URIBL) 137页面均有此选项。当这些选项中的指定文本相匹配时，该文本在邮件主题中只添加一次，即使该邮件满足每个选项下的条件。然而，如果您在一处或多处更改了文本，则同样也会添加该定制文本。因此，举个例子，若您在所有这三个选项下都将文本设置为 "SPAM*"，则该文本在主题中只会添加一次，而不管邮件是否匹配多个选项下的条件。不过，若您将 DNSBL 可选文本改为 "*DNS 阻止列表*"，在此选项和其他选项下邮件均符合标准，那么主题中将同时添加 "*垃圾邮件*"和 "*DNS 阻止列表*"。

...添加 [xx]点数到邮件总值
根据默认，未通过回呼验证检查的邮件，其邮件分数都将调整 1.0 分。您可以选择调整该值，或者若您不希望因为回呼验证而影响分值，您可禁用此选项。

即使 SecurityGateway 配置为接受邮件而不是拒绝或隔离邮件，但若邮件最终得分足够高，该邮件仍可能被拒绝或隔离，这取决于其他安全 124选项和邮件评分 143页上选项的配置。

例外

排除来自被列入允许列表的发件人的邮件
来自于 列入允许列表发件人[212] 的邮件根据默认不受回叫验证的检查。如果您不希望将已列入允许列表的发件人排除在回呼验证的需求之外，可禁用此选项。

排除来自经身份验证会话的邮件
根据默认，经由已验证会话发送的邮件排除在回呼验证的需求之外。即使会话已通过验证，您若还希望验证发件人，那么请不要勾选此框。

排除来自本地发件人的邮件
根据默认，来自于您本地发件人的邮件无需进行回呼验证。若您不希望排除本地收件人，请清理该选择框。

例外 - 域

当配置这些设置时，如果您在页面顶部的 *"针对域："* 下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。点击 *"查看/编辑"* 相应域的链接来查看或编辑其回呼验证设置，或者点击 *"重置"*，将域设置重置为默认的全局值。

4.3.7 发件人报头屏蔽

这个安全功能修改入站邮件的 "发件人："报头，来使报头的仅姓名部分包含姓名和邮件地址。这是为了抵御垃圾邮件和攻击中通常使用的策略，即伪装成邮件来自其他人。在显示邮件列表时，邮件客户端通常仅显示发件人的姓名，而不是姓名和邮件地址。要查看邮件地址，收件人必须先打开邮件或采取一些其他操作，例如右键点击条目或将鼠标悬停在姓名上等。出于这个原因，攻击者通常在可见的 "发件人"报头放置合法的人名或公司名称来构建邮件，并隐藏不合法的电子邮件地址。例如，一封邮件的实际 "发件人："报头可以是 "Honest Bank and Trust"<lightfingers.klepto@example.com>，但是您的客户端可能只将"Honest Bank and Trust"作为发件人显示。此功能会更改报头的可见部分来显示这两个部分。在上例中，现在会将发件人显示成 "Honest Bank and Trust (lightfingers.klepto@example.com)" <lightfingers.klepto@example.com>"，清楚为您指示这是伪造的欺诈邮件。

发件人报头屏蔽

为显示名添加电子邮件地址
如果您希望将入站邮件的 "发件人："报头的客户端可见部分修改成 包含发件人的姓名和邮件地址，请启用此项。会将新报头的结构从 "发件人姓名"<mailbox@example.com>更改成 "发件人姓名 (mailbox@example.com)"<mailbox@example.com>。默认情况下禁用此项，而且仅适用于指向本地用户的邮件。由于一些用户可能不希望修改 "发件人："报头，即使这有助于识别欺诈邮件，请慎用此项。

将邮件地址置于姓名前
在使用上方的 *"为显示名添加电子邮件地址"* 这个选项时，如果您希望在修改后的 "发件人："报头中交换姓名和电子邮件地址，请启用此项。使用上方示例，"Sender's Name" <mailbox@example.com> 现在将修改成："mailbox@example.com (发件人的姓名)"<mailbox@example.com>。

将显示名中不匹配的电子邮件地址替换为真实的电子邮件地址
垃圾邮件中使用的另一种策略是在 "发件人："报头的显示名称部分中添加了看似合法的姓名和电子邮件地址。即使它不是实际的发件电子邮件地址。如果您希望使用实际发件人地址替换此类邮件中的可见电子邮件地址，请使用此选项。例如："Frank's Company (frank@company.test)" <spoof@example.com> 将被更改成 "Frank's Company (spoof@example.com)" <spoof@example.com>.

例外

排除来自经身份验证会话的邮件
默认情况下，经由已验证会话发送的邮件排除在 "发件人报头屏蔽"设置之外。即使会话已通过验证，如果您还希望应用这些设置，那么请不要勾选此框。

排除来自域邮件服务器的邮件
默认情况下，来自于您其中一个域邮件服务器[66]的邮件无需受到 "发件人报头屏蔽"设置的限制。如果您仍然希望为来自那些服务器的邮件应用这些设置，请清除此选择框。

例外 - 域

当配置这些设置时，如果您在页面顶部的 *"针对域："* 下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。点击 *"查看/编辑"* 相应域的链接来查看或编辑其 "发件人报头屏蔽"设置，或者点击 *"重置"*，将该域的设置重置为默认的 "全局"值。

4.4 反滥用

安全[124]菜单下的 "反滥用"部分中包含了一些工具，帮助您防止别人滥用或者不恰当使用您的邮箱系统来中继垃圾邮件，使用大份额的带宽，过于频繁地连接至您的服务器，等等。 "反滥用"部分下有8个项目：

中继控制[173]—若收到一封邮件，它既不发往本地域，又非来自于本地域，便会询问 SecurityGateway 是否要代表第三方来发送或者中继该邮件。 "中继控制"页面上的设置决定了由谁来做这件事。 "中继控制"还具有一些选项，用于指定在 SMTP MAIL 或 RCPT 命令中通过的地址，当其包含了一个本地域时，该地址是否必须存在。

SMTP 验证[175]—该页面管理了 SMTP-AUTH 选项，从而扩展了 SMTP 的功能，在其中又包含了一个验证步骤。它实际上允许用户在发送邮件时登录服务器，从而确保用户身份是已知且有效的。SMTP 身份验证允许您跳过许多其他安全步骤，这些步骤旨在拦截垃圾邮件制造者和其他未经授权的用户，他们试图利用伪造的身份证明，通过您的服务器中转邮件。

IP 防护[176]—IP 防护是域名及其配套 IP 地址的列表，在 SMTP MAIL FROM 命令中会检查该列表。仅当发件服务器的 IP 地址与列于域中的某一经许可的 IP 地址匹配时，表明来自某一列出域里的发件人的 SMTP 连接才会获准。

动态屏蔽[177]—使用了该功能后，SecurityGateway 就可以跟踪发送方服务器的行为，以此来识别其可疑活动，然后作出相应的反应。例如，在与一个 IP 地址进行邮件会话时，一旦出现了特定数量的 "未知收件人"错误，那么您便可使用动态屏蔽来阻止该 IP 地址，使其今后无法连接至您的服务器。您可以阻止以下发件人：在指定时间内连接至您服务器的次数超出指定次数的发件人，以及未通过验证的次数超出指定次数的发件人。不过，动态屏蔽不是永久性的。只有在您指定的分钟数里，该 IP 地址是被阻止的，而且自从被阻止后，每一个 IP 地址以及通过的时间数均会列出。

位置屏蔽[178] - 是一种基于地理位置的阻止系统，您可以使用该系统阻止来自世界上未授权地区的入站连接。SecurityGateway 确定与连接 IP 地址关联的国家，然后阻止来自受限位置的连接。默认情况下，"位置屏蔽"只会阻止尝试进行身份验证的连接。例如，当您在特定国家/地区没有用户，但仍希望能够从那里接收邮件时，这很有用。这样您只会阻止那些试图登录到您服务器的尝试。

缓送[179]—一旦从邮件的发件人处收到指定数量的 RCPT 命令，采取缓送方式让您可以故意减缓连接。这是为了阻止垃圾邮件制造者试图向您的域发送未经请求的群发电子邮件（"垃圾邮件"）。您可指定启用缓送前允许的 RCPT 命令数，以及连接过程中每当从该主机接收到后续 RCPT 命令时延迟连接的秒数。该技术背后的推理是如果垃圾邮件制造者向您发送每封邮件都需要花费相当长的时间，这将迫使他们以后不再重复同样的操作。

带宽控制[180]—该功能让您能够监管 SecurityGateway 所消耗的带宽，全局和个别域皆可。通过使用 "带宽限制"，您可以控制每一个入站和出站 SMTP 会话的进程速率。此外，您可以让被列入允许列表的发件人、已验证的会话以及您的域邮件服务器免受这些限制。

账户劫持检测[181] - 此屏幕上的选项可用于检测服务器上可能被劫持的账户并自动阻止其发送邮件。例如，如果垃圾邮件发件人不知如何获得了一个账户的电子邮件地址和密码，然后该功能可以阻止垃圾邮件发件人使用此账户通过您的系统发送大量垃圾邮件。您可以指定在给定的分钟数内可由一个账户发送的最大邮件数量，并能选择在达到此限制时禁用这个账户。

QR 码检测[182] - QR网络钓鱼（也称为 "Qrshing"或 "Quishing"）是网络犯罪分子或诈骗犯有时使用的一种技术。他们将虚假的 QR 码附加到邮件中，试图让邮件接收者扫描代码，然后将其带到一个网站，该网站将用于从该人那里获取信息或进行其他诈骗。使用此页面上的选项，您可以配置 SecurityGateway，以便在将 QR 码图像附加到邮件时检测并采取行动。

4.4.1 中继控制

如果邮件并非发往或来自本地域，就会询问 SecurityGateway 以某些第三方的名义投递或中继邮件。SecurityGateway 不允许随便打开中继，但是如有必要，您可以使用该页的设置以允许您的域邮件服务器[66]使用中继功能。"中继控制"还具有一些选项，用于指定在 SMTP MAIL 或 RCPT 命令中通过的地址，当其包含了一个本地域时，该地址是否必须存在。

邮件中继

该服务器不 "中继"邮件...
SecurityGateway 不会中继那些既不发往也不来自其域的邮件，因为垃圾邮件发送者会使用打开中继的服务器以隐藏他们的骗术，因此随便地中继邮件会导致您的域被一个或多个 DNSBL[134] 服务列入阻止列表。

...除非发送自域邮件服务器
要是邮件既不发往也不来自您的域，但发自您的某一域邮件服务器[66]，如果您希望继续并中继邮件，请点击该选项。默认情况下，禁用该选项。

只有域邮件服务器才能发送本地邮件
默认情况下，当发件服务器作为一个本地域指定的某一域邮件服务器[66]时，SecurityGateway 将仅接收来自该域的邮件。如果您不希望限制本地邮件发送至每个域指定的邮件服务器，请清除该复选框。

……除非邮件发往本地帐户
在邮件指向本地账户，而您希望接收不是由您域邮件服务器[66]发送的本地邮件时请勾选此框。默认情况下，禁用该选项。

...除非通过已验证的 SMTP 会话发送
要是来自本地域的邮件没有被某一域所指定的邮件服务器发送，如果启用该选项并且发送中的这封邮件通过了已验证的会话，那么 SecurityGateway 仍将接收该邮件。比如，一个本地用户发送他的外发邮件时，是直接通过 SecurityGateway 而不是通过域邮件服务器的。默认情况下启用此项。

...除非发自列入允许列表的 IP 地址或主机
如果您希望允许从被列入允许列表[212]的 IP 地址和主机发送的本地邮件，即使发件服务器不是您的域邮件服务器[66]，请点击此项。默认情况下，禁用该选项。

账户验证

如果使用本地域，SMTP MAIL 地址必须存在
默认情况下，当邮件表明来自本地域时，SecurityGateway 将验证在 SMTP 过程中通过的 MAIL 值（比如，发件人）是否指向一个实际有效的帐户。如果该地址不存在，将拒收邮件。

……除非通过域邮件服务器发送
如果您希望将邮件从 *"SMTP MAIL 地址必须存在……"*选项中免除，（当发送中的邮件来自域邮件服务器[66]时），请启用该选项。默认启用此项。

...除非通过已验证的 SMTP 会话发送
当发送中的邮件通过已验证的 SMTP 邮件会话时，您希望将它们从 *"SMTP MAIL 地址必须存在……"*选项中免除，请启用该选项。默认情况下启用此项。

...除非发自列入允许列表的 IP 地址或主机
如果您希望将邮件从 *"SMTP MAIL 地址必须存在……"*选项中免除，（当发送中的邮件来自列于允许列表[212]的 IP 地址或主机时），请选中该选项。默认情况下，禁用该选项。

如果使用本地域，则 SMTP RCPT 地址必须存在
当邮件表明发往本地域时，SecurityGateway 将验证在 SMTP 过程中通过的 RCPT 值（例如收件人）是否指向一个实际有效的账户。如果该地址不存在，将拒收邮件。

4.4.2 SMTP 验证

该页上的设置管理 SMTP-AUTH，它扩展了 SMTP 以包括一条身份验证步骤。它实际上允许用户在发送邮件时登录服务器，从而确保用户身份是已知且有效的。SMTP 身份验证允许您跳过许多其他安全◆◆◆骤，这些步骤旨在拦截垃圾邮件制造者和其他未经授权的用户，他们试图利用伪造的身份证明，通过您的服务器中转邮件。

SMTP 验证

当邮件来自本地账户时，始终要求身份验证
若要求对任何号称来自本地账户的邮件都进行身份验证，请单击该复选框。若 SMTP 会话未通过身份验证，将拒绝该邮件。默认情况下，禁用该选项。

...除非邮件发往本地账户
当启用了上述*当邮件来自本地帐户时，始终要求身份验证*选项时，如果希望为收件人是本地账户的邮件免除该要求，请单击该选项。换句话说，当来自本地地址的邮件也发往本地地址时，不要求身份验证。默认情况下，禁用该选项。

...除非邮件来自于域邮件服务器
若希望为来自某个域邮件服务器[66]的邮件免除*当邮件来自本地帐户时，始终要求身份验证*这一操作，请单击该选项。

...除非邮件来自允许列表中的 IP 地址或主机
当邮件来自允许列表的 IP 地址[217]或主机[215]时，如果您希望免除 SMTP 身份验证要求中的本地账户，请选中此框。

身份验证凭证必须与电子邮件发件人的匹配
若要求发件人只能使用自己的凭证进行身份验证，请使用该选项。举例来说，*frank@example.com* 只能使用 *frank@example.com* 账户凭证进行身份验证。若他试图使用 *frank02@example.com* 进行身份验证，那么即使 *frank02@example.com* 凭证有效，也被禁止。默认情况下，禁用该选项。**请注意：**此项不应用于 SMTP AUTH 密码[43]。

发自“postmaster”、“abuse”和“webmaster”的邮件要求身份验证
当邮件声称来自本地域的 *postmaster*、*abuse* 或 *webmaster* 时，默认要求进行身份验证。这是因为许多垃圾邮件制造者和未经授权的用户知道服务器上存在着这些账户或别名，并试图利用它们中转邮件或伪装成这些可靠的地址。

不允许 SMTP 端口上的验证
如果启用了此项，当 SMTP 客户端提供了 AUTH 验证），则不会在 EHLO 响应中提供 AUTH，并且会将 AUTH 视为未知命令。此设置在所有合法账户都使用 MSA[76] 或其他端口来提交经过验证的邮件的配置中很有用。在这种配置中，假定在 SMTP 端口上进行任何验证的尝试都必须来自攻击者。

例外 - 域

当配置这些设置时，如果您在页面顶部的*“针对域：”*下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。点击相应域的*“查看/编辑”*链接以查看或编辑其 SMTP 身份验证设置，或点击*“重置”*将域设置重置为默认全局值。

4.4.3 IP 防护

IP 防护是一张域名与其相关 IP 地址的列表，在 SMTP MAIL FROM 命令中会进行检查。仅当发件服务器的 IP 地址与列于域中的某一经许可的 IP 地址匹配时，表明来自某一列出域里的发件人的 SMTP 连接才会获准。

配置

启用 IP 防护
勾选此框以启用 IP 防护功能。

对照 IP 防护数据库检查 FROM 报头。
如果您希望 "IP 防护"不仅比较取自 SMTP MAIL 值中的地址，还比较取自邮件 FROM 报头中的地址，请勾选此框。默认情况下，禁用该选项。

使用此项可能会对某些类型的邮件（例如那些来自邮件列表的邮件）造成问题。因此此项只有在您确实需要时才使用。

当前定义的域/IP 对

这是一张域与其相关 IP 地址的列表，当邮件表明来自某一列出的域时会检查 IP 地址。投递邮件服务器的 IP 地址必须列在相应的域中。

排除发往有效本地用户的邮件
默认情况下，当邮件地址是有效本地用户时，投递邮件的服务器将不顾 IP 防护的设置，不会被检查。如果您不希望在邮件地址是本地用户时将它们从 IP 防护中排除，请清除该复选框。

新建
要添加新的域/IP 地址条目到列表，请点击 *"新建"*。这将会打开 IP 防护条目页面。

编辑
要编辑现有的条目，双击该条目或者从列表中选中它并点击 *"编辑"*。这将会在 IP 防护条目页面打开该条目。

删除
要从列表删除条目，选中该条目并点击 *"删除"*。

IP 防护条目

域与 IP 信息

在创建新的 IP 防护条目或编辑现有的条目时会打开这个页面。

保存与关闭
在添加与编辑完域，IP 地址与任何相关 IP 防护条目的注释之后，请点击 *"保存与关闭"*来保存这些条目并返回至 IP 防护页面。

关闭
点击 *"关闭"*会直接返回到 IP 防护页面，不保存任何您在 IP 防护条目页面添加的信息与作出的修改。

域
在此输入您希望添加至 IP 防护的域名。

IP 地址
输入与以上列出的域相关联的 IP 地址。当邮件表明来自该域时，投递邮件的服务器的 IP 地址必须与之匹配。

备注
使用该区域列出任何与条目相关联的注释。

例外

排除发往有效本地用户的邮件
如果您希望在邮件地址指向有效本地用户时将它们从 IP 防护中排除，请勾选该复选框。

排除来自经身份验证会话的邮件
如果您希望在入站邮件来自经过验证的会话时，将其从 IP 防护中排除，请勾选此框。

排除来自域邮件服务器的邮件
默认情况下，来自域邮件服务器 66 的邮件将从 "IP 防护"排除。如果您希望将域邮件服务器从 "IP 防护"排除，请勾选该复选框。

4.4.4 动态屏蔽

使用了动态屏蔽特征后，SecurityGateway 就可以跟踪发件服务器的行为，以此来识别其可疑活动，然后作出相应的反应。例如，在与一个 IP 地址进行邮件会话时，一旦出现了特定数量的 "未知收件人"错误，那么您便可使用动态屏蔽来阻止该 IP 地址，使其今后无法连接至您的服务器。您可以阻止以下发件人：在指定时间内连接至您服务器的次数超出指定次数的发件人，以及未通过验证的次数超出指定次数的发件人。不过，动态屏蔽不是永久性的。阻止 IP 地址的时间就是您在此页面上所指定的分钟数，并且该页面底部的阻止 IP 列表中列出了每一个 IP 地址和自其被阻止后所通过的时间数。

自动 IP 屏蔽

启用动态屏蔽
点击此选项来激活动态屏蔽功能。根据默认，动态屏蔽已被禁用。

禁止导致多次 RCPT 尝试失败的发件人：
启用了动态屏蔽后，在 SMTP 会话过程中若来自于某一 IP 地址导致了指定数量的 RCPT 尝试失败，则将暂时阻止此地址。这是垃圾邮件发送者们常用的伎俩，发送许多 RCPT 命令，不过其中很多都是无效地址。该选项默认值为 10。

阻止在 [xx]分钟内链接超过 [xx]次的发件人。
该选项指定了某个人在指定的分钟数里所允许连接到 SecurityGateway 的次数。若在指定的时间内他们超过了连接数，则将暂时阻止发件人。默认情况下，禁用该选项。

禁止那些多次验证失败的发件人：
在将发件人暂时阻止以前，这是所能允许的发件人验证失败的次数。某人使用一个错误的密码，这就是一个会引起失败验证尝试的示例。根据默认，若发件人三次验证失败，那么其 IP 地址将被暂时阻止。若您不希望阻止这些发件人，不论他们的失败尝试数是多少，请清除此选择框。

禁止发件人这些分钟：
若邮件违反了下列的一条限制，将暂时阻止发件人，这是此 IP 地址将被阻止的分钟数。IP 地址将被阻止的默认时间长度为 10 分钟。

禁止发件人后关闭 SMTP 会话
当一个 IP 地址被阻止后，根据默认 SMTP 会话将被立刻关闭。换句话来说，该会话将不允许继续进行正常 SMTP 协议的后续步骤，连接将被切断。若您不希望立刻终止与一个受阻止的 IP 地址的连接，请清除此选择框。

例外

排除发自被列入允许列表的 IP 地址和主机的邮件
根据默认，所有已列入允许列表的 212 IP 地址和主机无需受到动态屏蔽的限制。如果您希望这些已列入允许列表的 IP 和主机也要遵守这些限制的话，请清除此选择框。

排除来自经身份验证会话的邮件
若一封入站邮件来自于一个已验证的会话，那么根据默认，它将无需受到动态屏蔽的限制。如果您希望这些限制同样应用于已验证的会话，请不要勾选此框。

排除来自域邮件服务器的邮件
根据默认，来自于您其中一个域邮件服务器 66 的邮件无需受到动态屏蔽的限制。若您不希望将域邮件服务器排除在动态屏蔽的限制之外，请清除该选择框。

已阻止的 IP 列表

该区域列出了目前受到阻止的所有 IP 地址以及每封邮件从被阻止以后所经过的时间数。从列表中选中条目，然后点击列表上方工具栏中的删除按钮，即可删除该条目。

4.4.5 位置屏蔽

位置屏蔽

“位置屏蔽”是一种基于地理位置的阻止系统，您可以使用该系统阻止来自世界上未授权地区的入站连接。SecurityGateway 确定与连接 IP 地址关联的国家，然后阻止来自受限位置的连接。默认情况下，“位置屏蔽”只会阻止尝试进行身份验证的连接。例如，当您在特定国家/地区没有用户，但仍希望能够从那里接收邮件时，这很有用。这样您只会阻止那些试图登录到您服务器的尝试。

启用位置屏蔽
要使用“位置屏蔽”，请启用此项，并点击您想要屏蔽的任何区域或国家旁边的框，然后点击“保存”。复选框表示将阻止来自该地区或国家/地区的所有连接，但您明确排除在此限制之外的任何 IP 地址除外（请参阅下方的例外项）。如果您再次点击某个框，则复选标记将更改为破折号。对于这些地区或国家/地区，SMTP 邮件连接将被接受，但尝试进行身份验证的连接将被阻止。当您希望能够接收来自某个国家/地区的电子邮件，但知道您在该国家/地区没有用户时，这可能很有用，这意味着从该国家/地区向您的服务器进行身

份验证的任何尝试都是欺诈性的，并且可能是暴力或字典攻击的一部分。最后，值得注意的是，无法为任何被封锁国家/地区的收件人使用安全通信[90]，因为他们将无法连接到 SecurityGateway 来查看安全的邮件。

为邮件添加 "X-SGOrigin-Country"报头
默认情况下，在启用 "位置屏蔽"时"，SecurityGateway 会将 "X-SGOrigin-Country"报头插入邮件，来进行内容过滤或用于其他目的。该报头包含双字母的 ISO 3166 国家和洲代码，而不是全名。如果您不希望插入该报头，请清除该复选框。

选择/取消全选
使用这些按钮来选择或取消选择列表中的所有位置。

例外

排除列于允许列表的 IP 地址的连接
根据默认，所有已列入允许列表的[217] IP 地址和主机无需受到 "位置屏蔽"的限制。如果您希望将 "位置屏蔽"应用到列入允许列表的 IP，请清除此复选框。

例外 - 域

当配置这些设置时，如果您在页面顶部的 *"针对域："* 下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。点击 *"查看/编辑"* 相应域的链接来查看或编辑其 "位置屏蔽"设置，或者点击 *"重置"*，将域设置重置为默认的全局值。

4.4.6 缓送

使用缓送 (Tarpitting)技术，一旦从邮件收件人处收到指定数量的 RCPT 命令，则可以有意减缓连接速度。这是为了阻止垃圾邮件制造者试图向您的域发送未经请求的群发电子邮件（"垃圾邮件"）。您可指定启用缓送前允许的 RCPT 命令数，以及连接过程中每当从该主机接收到后续 RCPT 命令时延迟连接的秒数。该技术背后的推理是如果垃圾邮件制造者向您发送每封邮件都需要花费相当长的时间，这将迫使他们以后不再重复同样的操作。

缓送设置

激活缓送
点击该复选框激活缓送 (Tarpitting)功能。默认情况下禁用缓送。

SMTP EHLO/HELO 延时 (以秒为单位)：
使用该选项延迟 SecurityGateway 对 EHLO/HELO SMTP 命令的响应。延迟响应哪怕 10 秒钟也可能会节省大量处理时间，因为它减少了收到的垃圾邮件数量。垃圾邮件制造者常常依赖于邮件的快速投递，因此不会长时间等待对 EHLO/HELO 命令的响应。使用哪怕很小的延时，有时会使垃圾邮件制造工具放弃等待响应而继续群发操作。MSA 端口 (在电子邮件协议[76]页面上指定)的连接都不受该延迟的限制。该选项的默认设置是 "0"，表示不会延迟 EHLO/HELO 响应。

经过身份验证的 IP 每天经历一次 HELO/EHLO 延迟
指定了 EHLO/HELO 延迟后，IP 地址 (其上建立了经过身份验证的 SMTP 会话)每天只经历一次延迟。该延迟直接发生在对会话进行首次身份验证之前。默认情况下，禁用该选项。

SMTP RCPT 缓送 (tarpit)阈值
使用该选项指定 SecurityGateway 开始缓送或延迟给定主机前在邮件会话期间允许该主机发送的 SMTP RCPT 命令数。例如，如果该阈值设为 10 且发送主机试图将邮件发送到 20 个地址 (即 20 条 RCPT 命令)，那么 SecurityGateway 将允许正常处理前 10 条命令，而在之后的每条命令后暂停以下 *SMTP RCPT 缓送延时*选项中指定的秒数。该选项默认值为 5。

SMTP RCPT 缓送延时 (以秒为单位)：
一旦达到某主机的 *SMTP RCPT 缓送阈值*，SecurityGateway 即在与该主机的邮件会话期间收到的每条后续 RCPT 命令后暂停这些秒数。每条后续 RCPT 命令默认延迟 10 秒钟。

缩放系数：
基本缓送延时随时间按此倍数增加。当达到缓送阈值且将缓送延时应用于会话时，每一延时将与该值相乘以确定会话中的下一延时长度。例如，如果缓送延时设为 10 而缩放系数设为 1.5，那么第一个延时将为 10 秒钟，第二个延时为 15 秒钟，第三个延时 22.5 秒钟，然后是 33.75，依此类推 (即 10 x 1.5 = 15，15 x 1.5 = 22.5 等等)。. 默认缩放系数为 1，意味着延时不会增加。

例外

排除来自被列入允许列表的发件人的邮件
默认情况下，来自允许列表[212]发件人的所有邮件不受缓送约束。若希望被列入允许列表的发件人也受缓送规则约束，请清除该复选框。

排除来自经身份验证会话的邮件
默认情况下，来自经身份验证会话的邮件不受缓送约束。若取消选中该复选框，则缓送约束同样应用于这些邮件。

排除来自域邮件服务器的邮件
默认情况下，来自域邮件服务器[66]的邮件不受缓送约束。若希望域邮件服务器接受缓送规则的约束，请清除该复选框。

4.4.7 带宽限制

"带宽限制"帮助您监管 SecurityGateway 所消耗的带宽，全局和个别域皆可。通过使用"带宽限制"，您可以控制每一个入站和出站 SMTP 会话的进程速率。此外，您可以让被列入允许列表的发件人、已验证的会话以及您的域邮件服务器免受这些限制。"带宽限制"系统根据每秒的千字节来校准，入站与出站的 SMTP 会话默认值均为 10 (虽然根据默认这两项都已禁用)。

在带宽限制起作用之前，最多可发送/接收 8 千字节的数据。因此这样会超出您的限制，这取决于你所指定的以下数目大小。

带宽限制

将入站 SMTP 连接限制为：[xx]KB/秒
如果您希望限制入站 SMTP 会话的带宽，请选择该选项。该选项的默认值为 10 千字节/秒，但是根据默认已禁用。

将出站 SMTP 连接限制为：[xx]KB/秒
如果您希望限制出站 SMTP 会话的带宽，请选择该选项。该选项的默认值为 10 千字节/秒，但是根据默认已禁用。

例外

排除来自被列入允许列表的发件人的邮件
如果您希望所有的被列入允许列表的发件人[212]不受带宽控制的限制，请启用此选项。默认情况下，禁用该选项。

排除来自经身份验证会话的邮件
如果一段会话已经验证，您欲使其免受带宽控制的限制，请使用此选项。默认情况下，禁用该选项。

排除域邮件服务器
如果您希望所有的域邮件服务器[66]不受带宽控制的限制，请勾选此框。默认情况下，禁用该选项。

例外 - 域

当配置这些设置时，如果您在页面顶部的 *"针对域："* 下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。点击 *"查看/编辑"* 相应域的链接来查看或编辑其带宽控制设置，或者点击 *"重置"*，将域设置重置为默认的全局值。

4.4.8 账户劫持检测

账户劫持检测

此屏幕上的选项可用于检测服务器上可能被劫持的账户并自动阻止其发送邮件。例如，如果垃圾邮件发件人不知如何获得了一个账户的电子邮件地址和密码，然后该功能可以阻止垃圾邮件发件人使用此账户通过您的系统发送大量垃圾邮件。您可以指定在给定的分钟数内可由一个账户发送的最大邮件数量，并能选择在达到此限制时禁用这个账户。您可以启用 *从 "账户劫持检测"免除此账户* 这个选项（位于 "账户设置"页面[31]）来从 "账户劫持检测"中免除特定的用户。您可以在用户选项[60]页面上为特定的用户选项设置默认值。

"账户劫持检测"仅适用于已验证会话中的本地账户，并自动免除邮件管理员账户。

账户可以在 [xx]分钟内发送不超过 [xx]封邮件
如果您希望阻止本地账户在指定的分钟数内发送超过指定数量的邮件，请使用此项。如果一个账户尝试发送超过指定数量的邮件，SecurityGateway 虽然不会断开连接，但是将使用 452 错误拒收超出限制的邮件直到时间限制期满。然后 MDaemon 才会再次接收来自此账户的邮件。

在达到限制时禁用账户
如果您希望禁用尝试发送超过指定数量邮件的账户，请勾选此框。发生上述情况时，服务器将发送 552 错误，断开连接，并立即禁用该账户。被禁用的账户不再能发送邮件或检查其邮件，不过 SecurityGateway 将仍然为此账户接收入站邮件。而且在禁用

账户时，会向邮件管理员发送一封有关此账户的电子邮件。如果邮件管理员希望重新启用此账户，他只需回复这封邮件即可。

例外 - 域

当配置这些设置时，如果您在页面顶部的 *"针对域："* 下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。点击相应域的 *"查看/编辑"* 链接以查看或编辑其 "账户劫持检测"设置，或点击 *"重置"* 将域设置重置为默认全局值。

4.4.9 QR 码检测

QR 网络钓鱼（也称为 "QRshing"或 "Quishing"）是网络犯罪分子或诈骗犯有时使用的一种技术。他们将虚假的 QR 码附加到邮件中，试图让邮件接收者扫描代码，然后将其带到一个网站，该网站将用于从该人那里获取信息或进行其他诈骗。使用此页面上的选项，您可以配置 SecurityGateway，以便在将 QR 码图像附加到邮件时检测并采取行动。

配置

启用 QR 码检测
点击此项来启用 QR 码检测。

当在邮件中找到附加的 QR 码时：

...拒收邮件
如果您希望 SecurityGateway 在附加 QR 码时拒收邮件，请选择此选项。

...隔离邮件
如果您希望在发现附加了 QR 码时隔离邮件，请选择此选项。选择此选项后，您还可以使用下面的 "标记主题"和 "添加点数到"选项。

...接受邮件
如果您希望在发现附加了 QR 码时接收邮件，请选择此选项。然后，您可以使用下方的 "标记主题"和 "添加点数到"选项来标记该邮件，或使用 SecurityGateway 的过滤[195]和反垃圾邮件[143]选项来采取其他操作。

...以 [*QR 码 ***] 来标记主题**
当您选择隔离或接受附加了 QR 码的邮件时，您可以使用此选项向邮件的主题报头添加一些文本。然后您可以有选择性地使用 SecurityGateway 的过滤[195]选项来基于添加的文本采取某些操作。

...添加 [xx] 点数到邮件总值
当您选择隔离或接受附加了 QR 码的邮件时，您可以使用此选项向邮件分值添加点数，这可以基于邮件分值[143]设置采取某些操作。默认情况下，此选项将 2.0 点数添加到 "邮件分值"。

例外

排除来自被列入允许列表的发件人的邮件
如果您希望所有的被列入允许列表的发件人[212]不受 QR 码检测的限制，请启用此选项。默认情况下启用此项。

排除来自经身份验证会话的邮件
如果您希望在会话通过身份验证时从 QR 码检测中排除会话，请使用此选项。默认情况下启用此项。

排除域邮件服务器
如果您希望域邮件服务器[66]不受 QR 码检测的限制，请勾选此框。默认情况下启用此项。

例外 - 域

当配置这些设置时，如果您在页面顶部的 *"针对域："* 下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。请点击相应域的 *"查看/编辑"* 链接以查看或编辑其 "QR 码检测"设置，或点击 *"重置"* 将域设置重置为默认全局值。

4.5 RMail™

RMail™ 是 RPost® 提供的服务，它的使用很直观，并不需要你的收件人有任何特殊的软件。RMail为所有行业和部门的各种规模的消费者和企业提供电子邮件使用。

RMail服务由 RPost 的 Registered Email技术提供支持，该技术是电子邮件投递证明的全球标准。RMail服务扩展了您的电子邮件平台，它提供：

- 跟踪您重要的电子邮件，知道它们投递和打开的时间。
- 投递证明、时间和准确内容。
- 轻松加密敏感的电子邮件和附件来确保安全或法律合规。
- 为通过电子签署文件来完成交易的各方提供简单方法。

使用试用的 RPost 账户，每个用户每月只能收发 5 封加密邮件。可以通过 RPost 购买额外的邮件。请前往 RPost.com 来了解增加邮件限制的规划/价格信息。

可以从 "安全"菜单下的 RMail页面[183]来启用和配置 Rmail服务。可以将其作为邮件内容过滤器规则中的操作[199]实施。

加密

启用 RMail加密服务
如果您希望将 RMail的加密服务用于邮件，请选中此框。您可以将 SecurityGateway配置为对所有邮件或仅具有以某个指定关键字开头主题的邮件使用 RMail加密。

排除日历邀请
如果您希望从 RMail处理中排除日历邀请邮件，请选中此框。

加密所有邮件
如果您希望对所有邮件使用 RMail加密，请选择此选项。

仅加密这些邮件...
如果您希望仅对那些主题以下面指定的关键字开头的邮件使用 RMail加密，请选择此选项。

加密主题开头为以下项的邮件...
选定上方的 *"仅加密这些邮件..."*时，RMail加密将用于具有以这些指定关键字之一为主题开头的邮件。使用添加/删除按钮来管理关键字。

删除主题中的匹配标记
如果您希望从触发 RMail处理的邮件中删除匹配的主题标签，请选中此框。

加密邮件，如果邮件发往...
如果您希望加密发送给某些收件人的邮件，请使用此选项。

跟踪 & 证明

启用 RMail跟踪 & 证明服务
如果您希望将 RMail的 Registered Email(注册邮件)技术服务用于邮件，请选中此框。您可以配置 SecurityGateway 为所有邮件或仅包含某些指定关键字的邮件执行此操作。这允许用户跟踪他们的邮件，接收时间戳报告来证明邮件何时被投递和打开。

排除日历邀请
如果您希望从 "RMail跟踪 & 证明"服务中排除日历邀请邮件，请选中此框。

跟踪所有邮件
如果您希望为所有邮件使用 RMail的跟踪和证明选项，请选择此选项。

仅跟踪这些邮件...
如果您希望仅为包含下面指定的其中一个关键字的邮件使用 RMail跟踪和证明选项，请选择此项。关键字可以位于邮件的主题报头或正文中。

在邮件主题或正文包含以下项时跟踪邮件...
在选定上方的 *"仅跟踪这些邮件..."*时，RMail的跟踪和证明选项将用于在主题或正文中包含这些单词之一的邮件。使用添加/删除按钮来管理指定的关键字。

删除主题中的匹配标记
如果您希望从触发 RMail跟踪和证明的邮件中删除匹配的主题标签，请选中此框。

电子签名

启用 RMail电子签名服务
如果您希望将 RMail的电子签名服务用于电子签名文档，请选中此框。您可以配置 SecurityGateway 为所有邮件或仅包含某些指定关键字的邮件执行此操作。

排除日历邀请
如果您希望从 "RMail电子签名"服务中排除日历邀请邮件，请选中此框。

签名所有邮件
如果您希望以电子方式签名所有邮件，请选择此选项。

仅签名这些邮件...
如果您希望仅电子签名包含下列指定关键字之一的邮件，请选择此选项。关键字可以位于邮件的主题报头或正文中。

在邮件主题或正文包含以下项时签名邮件...
在选定上方的 *"仅签名这些邮件..."*时，RMail的电子签名选项将用于在主题或正文中包含这些单词之一的邮件。使用添加/删除按钮来管理指定的关键字。

删除主题中的匹配标记
如果您希望从触发 RMail电子签名的邮件中删除匹配的主题标签，请选中此框。

4.6 数据泄露防护

"数据泄露防护"功能基于邮件内容过滤器[195]系统，可用于创建过滤规则以查找包含特定种类敏感信息的邮件，然后阻止投递这些邮件。其中为您提供大量全局规则来搜索一下数据，例如：信用卡号码、银行账户信息和护照号码等。当您启用这些规则时，默认情况下它仅适用于出站邮件，并在规则匹配时向管理隔离[256]发送邮件。包含的规则可以像任何其他规则一样进行管理和修改。

使用此页面来管理您的 "数据泄漏防护规则"。您可在此处创建，编辑或者删除您的规则，只需点击条目中的一个选择框，您即可快速地启用或者禁用任意规则。就像 "邮件内容过滤"规则一样，"数据泄漏防护"规则可用于指定 SecurityGateway 将对其处理的每条邮件进行测试的特定标准。接着，若邮件符合一项规则，便可执行一系列的操作。您可以创建规则来查看特定报头是否存在，查看特定发件人或收件人，在报头或者邮件正文搜索特定文本，测试邮件的大小，以及很多其他操作。若一封邮件符合一条规则的测试，那么此项规则可导致邮件被拒收，删除，隔离，复制或者重定向至不同的地址，等等。

"数据泄露防护"规则列表有三栏：启用，描述及预览。启用栏里包含了一个每个条目的选择框，可以用来快速地启用/禁用规则。描述栏中包含了 *"规则名称"*，是由您在创建一条规则时所指定的。预览栏中包含了每条规则的图标，当您将指针悬停在某一规则时，将显示该规则的工具提示。工具提示中包含了真正的 Sieve 脚本[219]，该脚本由数据泄露防护规则编辑器[186]创建，用来为规则而服务。

页面顶部的工具栏包含了下列四个选项：

新建
点击 *"新建"*来打开数据泄露防护规则编辑器[186]，用来创建一条新规则。

编辑
选中一条规则然后点击工具栏上的 *"编辑"*，并在数据泄露防护规则编辑器[186]中将其打开。或者，您只需双击一条规则将其打开。

删除
要删除一条或多条规则，从列表中选中条目然后点击 *"删除"*。会跳出一个框，要求您确认是否决定删除规则。您可以使用 "Ctrl和 Shift"键来选择多个条目。

针对域：
使用 *"针对域："*通过下拉列表框来选择在列表中要显示哪条规则。您可显示全局规则，该规则适用于一切域，或者您可以显示特定域的规则。

数据泄露防护规则编辑器

数据泄露防护规则编辑器用于创建新规则或者编辑现有规则。欲创建一条新规则，点击 "数据泄露防护规则"工具栏上的*新建*，然后逐一（顶部到底部）进入编辑器选项，每次只进入一个选项。完成后，点击 *"保存并关闭"*来创建新规则。

已启用该规则
要创建一条新规则，必须勾选此框。至于现有的规则，您可以取消勾选此框将此规则禁用。在测试邮件时，SecurityGateway 不会使用已禁用的规则。该选项所对应的是 "数据泄露防护规则"列表上的 *"启用"*栏。

针对域：
使用此选项来选择该规则所适用的域。如果选择了 "--全局--"，那么发送至或者来自于您 SecurityGateway 的一切域的全部邮件都将按照该规则进行测试。如果选择的是一个特定域，那么只需测试发送至或来自于该特定域的邮件。

规则名称：
在此输入规则的描述性名称。该选项所响应的是 "数据泄露防护规则"列表上的 *"描述"*栏。

应用此规则，如果

所有条件都符合（与）
如果您希望只有当一封邮件满足了所有您所提供的如下测试条件后再匹配一条规则的话，请选择此选项。这是在测试条件下执行一个合乎逻辑的 "与"。换句话来说，"若条件 A 是真的且条件 B 也是真的，那么就执行特定操作。"

...大约 [xx] 字符数以内
启用此项时，仅在*待比较项目*是正文时才应用，其中还包括 SecurityGateway 能够从中提取文本的附件。如果正文存在多个条件，那么所有这些条件都必须在彼此的指定接近度（之前或之后的字符数）内找到。匹配必须全部发生在同一个 mime 部分中，即邮件正文、备选正文或附件。在 "AND"中包含的其他条件必须为 true，不过无需彼此接近。

符合任意条件（或）
如果您希望一封邮件满足了您所提供的如下测试条件中的任意一项后再匹配一条规则的话，请选择此选项。这是在测试条件下执行一个合乎逻辑的 "或"。换句话来说，"若条件 A 是真的或者条件 B 是真的，那么就执行特定操作。"

条件：
该框显示您为规则提供的所有当前测试条件。点击框中的条件，您可以编辑任意一项。点击紧靠条件旁边的**[Remove]**，您可以删除任意一项。

添加条件
请点击 "**添加条件**"来新建一个条件，以便添加到该规则当前的*条件*列表中。添加完条件后，您可通过再次点击该链接来添加更多条件。有关不同类型条件的更多信息，还请参阅下方的规则条件 187。

操作：
当一封邮件符合规则条件时，从此列表中选出您希望执行的操作。若选中操作需要更多数据，在此操作下会出现一个相应的控件让您输入该数据。欲获得您可以执行的不同类

型操作的信息，请见下方的操作[190]。当您为您的规则设置完所有条件并且选中了一项操作后，请点击 *"保存并关闭"*来关闭编辑器并在列表中添加新规则。

规则条件

当您希望给一条规则添加一个测试条件时，您将会使用 *"点击此处为该规则添加一个条件"*链接来打开规则条件这一屏幕。在使用该屏幕来创建测试条件时，您必须首先指定邮件属性，或者您欲进行测试或比较的项目。接着，您必须指定如何测试或比较此项目：该项目是否包含特定文本，它是否完全等同于特定文本，是否存在特定的报头，等等。有若干可被测试的项目，并有多种常见的测试方法。当您已选中项目、测试方法且已输入任何所需信息，请点击 *"保存并关闭"*从而向您的规则中添加测试条件。

要比较的项目：
这些是您可以在邮件中测试的项目。

- **MAIL (From)** —该测试使用的值就是 SMTP "MAIL From"命令所通过的值。这就表明了邮件从何而来，不过并不一定要与邮件的 "发件人"报头所包含的信息完全一致。有时 "发件人"报头会包含额外信息或者不同信息。除了那九种常见的测试或比较项目的方法之外 (见下)，该项目同样可以进行比较，使用 "是本地用户"和 "非本地用户"测试。
- **RCPT (To)** — 该测试使用的值就是 SMTP "RCPT To"命令所通过的值。这就表明了邮件从何而来，不过并不一定要与邮件的 "收件人"报头所包含的信息完全一致。有时 "收件人"报头会包含额外信息或者不同信息。除了那九种常见的测试或比较项目的方法之外 (见下)，该项目同样可以进行比较，使用 "是本地用户"和 "非本地用户"测试。
- **MAIL and RCPT** —选择此项目来使用 SMTP "MAIL From"和 SMTP "RCPT To"命令来确定邮件是入站、出站还是内部邮件 (请参阅下方的 *"额外测试方法"*)。
- **IP**—选择该项目来测试发件服务器或客户端的 IP 地址。
- **HEADER** — 如果您希望指定一个要比较的报头，请选择该项目。若选中，将出现一个 *"报头名称"*选项，让您指定对于此测试条件，将使用哪个报头。除了那九种常见的测试项目的方法之外，该项目同样可以进行比较，使用 "报头存在"以及 "报头不存在"测试。**注意：**在指定 *"报头名称"*时，在报头名称里不要使用冒号。例如，使用 "发件人"作为 *"报头名称"*，而不用 "发件人："，若您希望比较发件人报头。
- **SUBJECT** —这是邮件的 "主题"报头。若您希望测试邮件的主题，请选择该项目。
- **BODY** — 选择 *"正文"*，若您希望使用邮件正文作为测试项目来比较。
- **BODY or SUBJECT** —在 *"正文"*或 *"主题"*匹配此规则条件时，如果您希望创建一个为 true 的规则，请选择此项目。这个项目是为了简化规则创建而提供的，因为它实际上等同于创建具有两个单独 "OR"语句的规则，一个搜索 *"正文"*，另一个搜索 *"主题"*来查看是否存在相同的文本。
- **ENVIRONMENT (SecurityGateway)** — 如果希望测试条件基于 SecurityGateway 的环境因素，请选择此项，例如：邮件是否来自域邮件服务器[66]，发件人是否经过验证，是否位于允许列表[212]或阻止列表[205]，邮件分值[143]是否大于或等于指定的分数，是否邮件被标记为已隔离（用户）[255]或已隔离（管理员）[256]。

如何比较：
此列表中包含了可用来测试或比较项目的方法，这些项目是在 *"上述想比较的对象"*选项里选中的。对于所有项目来说，有多种常见的测试方法。MAIL and RCPT 与 ENVIRONMENT (SecurityGateway) 项目有独特的比较程序集，Mail(From)、RCPT(To) 和 Header 有额外的测试方法。

常见的测试方法：
这些测试方法每一种都是将上述要比较的项目中选中的项目与*您在下方所指定的如何比较中所选中方法*的搜索值相比较。这些类型的比较都对上方的 *"待比较项目"*选项可用，MAIL、RCPT 和 ENVIRONMENT (SecurityGateway) 除外。他们每个人都有一组独特的比较程序。

- **包含** — 若选中了此方法，如果 *"搜索值"*是一个子字符串或是*上述指定的要比较项目的一部分*，那么该比较符合条件或者是 "true"。例如，若您选择了 "MAIL (From)"作为要比较的项目，然后选择 "包含"作为比较的方法，以 "example.com"作为 *"搜索值"*，那么来自于含有 "example.com"地址的任意一封邮件都将符合该条件。
- **不包含**—若选中了此方法，如果 *"搜索值"*不是一个子字符串，也不是*上述指定的要比较项目的一部分*，那么该比较符合条件或者是 "true"。例如，若您选择了 "MAIL (From)"作为要比较的项目，然后选择 "不包含"作为比较的方法，以 "example.com"作为 *"搜索值"*，那么除了那些含有 "example.com"地址的邮件外，其他任意一封邮件都将符合该条件。
- **包含文字** — T此比较器类似于 "包含"，不过仅在字边界锚跟随在此字符串后面时才匹配。这避免了需要手动创建以下格式：\b(word1|word2|word3)\b。例如：一个规则搜索*包含* "cat"的邮件正文时，只有邮件包含完整的 "cat"时才匹配。如果邮件包含 *catfish* 或 *certificate* 则不匹配。
- **不包含文字**—T此比较器类似于 "不包含"，不过仅在不存在含有跟随在此字符串后的字边界锚的字符串时才匹配。例如：一个规则搜索*不包含* "cat"的邮件正文时，将匹配不包含完整 "cat"的任何邮件，即使正文包含 *catfish* 或 *certificate* 时也匹配。
- **等于**—此方法与上述的 *"包含"*类似，不同之处在于 *"搜索值"*必须与 *"要比较项目的值"*完全匹配，而不是仅仅是该值的一部分。例如，若您选择了 IP 作为要比较的项目，然后选择 "等于"作为比较的方法，以 "192.168.0.1"作为 *"搜索值"*，那么只有来自于该准确 IP 地址的邮件才符合条件。
- **不等于**—此类型的比较与先前的方式正好相反。如果 *"要比较项目的值"*与 *"搜索值"不完全相同*，那么该比较是真的。例如，若您选择了 IP 作为要比较的项目，然后选择 "等于"作为比较的方法，以 "192.168.0.1"作为 *"搜索值"*，那么除了那些来自于该准确 IP 地址的邮件外，其他任意一封邮件都符合条件。
- **以...开头** — 当 *"搜索值"*与上述所指定的要比较项目的值开头相符时，*若您希望考虑一个条件为 True*，那么请使用此类型的比较。例如，若您选择 *"主题"*作为要比较的项目，"[allstaff]"作为搜索值，那么所有主题行以 "[allstaff]"开头的邮件都符合条件。
- **不以...开头**—与先前的比较类型正好相反。当 *"搜索值"*与上述所指定的要比较项目的值开头不相符时，*若您希望考虑一个条件为 True*，那么请使用此选项。例如，若您选择 *"主题"*作为要比较的项目，"[allstaff]"作为搜索值，那么除了主题行以 "[allstaff]"开头的邮件以外，其他任意邮件都符合条件。
- **以...结尾**—该比较指的是每当 *"要比较项目的值"*以 *"搜索值"*作为结尾，即符合

了条件。例如，若您选择了 RCPT (To) 作为要比较的项目且将 "以...结尾"作为比较方法，以 "cn"作为搜索值，那么以 "cn"作为邮件地址结尾的全部邮件都将符合条件。

- **不以...结尾**—该比较指的是每当 *"要比较项目的值"*不以 *"搜索值"*作为结尾，即符合了条件。例如，若您选择了 RCPT (To) 作为要比较的项目且将 "以...结尾"作为比较方法，以 "cn"作为搜索值，那么除了以 "cn"作为邮件地址结尾的全部邮件之外，其他任意邮件都将符合条件。
- **匹配正则表达式**—如果您希望在以下情况使用正则表达式，即比较在上方 *"特比较项目"*这一选项中选定的项目，请选择此项。

额外的测试方法：

- **是本地用户**—该比较方法只适用于上述的 MAIL (From) 以及 RCPT (TO) 选项。当邮件地址是本地的 SecurityGateway 用户时，若您希望符合条件或条件为 "true"，请选择此选项。例如，若您选择 MAIL (From) 作为 *"要比较的项目"*，那么只有来自于本地用户的邮件才符合条件。
- **非本地用户**—该比较方法只适用于上述的 MAIL (From) 以及 RCPT (TO) 选项。当邮件地址不是本地的 SecurityGateway 用户时，若您希望符合条件或条件为 "true"，请选择此选项。例如，若您选择 MAIL (From) 作为 *"要比较的项目"*，那么来自于远程用户的所有邮件都符合条件。
- **报头存在**—只有当您选择 "报头"作为 *"要比较的项目"时*，此选项才可用。当您选择了此选项并且在 *"所提供的选项中"*指定了报头的名称，只有当邮件中出现指定报头时才符合条件。例如，若您指定了 "X-我的-自定义-报头"作为 *"报头名称"*，那么所有显示该报头的邮件都符合条件。无此报头的任意一封邮件都不符合条件。
- **报头不存在**—只有当您选择 "报头"作为 *"要比较的项目"时*，此选项才可用。当您选择了此选项并且在所提供的选项中指定了 *"报头名称"*，只有当邮件中不显示指定报头时才符合条件。例如，若您指定了 "X-我的-自定义-报头"作为 *"报头名称"*，那么所有不显示该报头的邮件都符合条件。显示此报头的任意一封邮件都不符合条件。
- **邮件是/不是[入站 | 出站 | 内部]**—这些比较程序仅适用于MAIL and RCPT项目。SMTP "MAIL From"和 SMTP "RCPT To"值都用于确定邮件是否为入站，出站或内部邮件。
  - **入站**—邮件是指向本地用户的，而不是来自同一个域的本地用户。
  - **出站**—邮件是来自本地用户的，而不是指向同一个域的本地用户。
  - **内部**—邮件来往于同一个域的本地用户。
- **ENVIRONMENT (SecurityGateway) 测试方式** — 以下测试方法仅适用于在您选择了 ENVIRONMENT (SecurityGateway) 作为 *"特比较项目"*的时候：
  - **域邮件服务器** — 该邮件来自或不来自您的域邮件服务器 66。
  - **已验证发件人**— 选择此项，可根据发件人是否经过身份验证来设置条件。
  - **发件人位于[允许列表 | 阻止列表]**— 是否是位于允许列表 212或阻止列表 205上的发件人。
  - **邮件分值（大于或等于）**— 使用此项来基于邮件分值 143设置规则。

- **已标记邮件：[已隔离（用户）| 已隔离（管理员）]** — 按照邮件是否被标记为已隔离（用户）255或已隔离（管理员）256来设置条件。

操作

待为您的规则设置完所有条件后，使用“规则编辑器”上的“*操作*”选项来选择当一封邮件符合规则条件时所要执行的操作。有七种操作可供选择：

- **拒收** — 若您希望拒收一封符合该规则内条件的邮件，请选择此操作。当选中了该选项时，在操作下方会出现一个“*SMTP 反应*”选项，您可以指定在邮件拒收时所发送的文本反应。例如，在“*SMTP 反应*”选项中，若您使用了，“我们不需要你的垃圾邮件！”，在 SMTP 会话过程中，当 SecurityGateway 拒收一封符合规则的邮件时，它将会发送“550 我们不要你的垃圾邮件。”
- **删除** —当一封邮件符合规则的条件时，该操作将使邮件被删除。与“拒收”操作不同的是，该选项不会发送 SMTP 反应，也不会发送投递失败邮件，就单纯地将邮件删除。
- **隔离** —若选中了该操作，如果收件人是本地用户，那么符合该规则下条件的邮件将置于收件人的隔离255中。如果收件人是远程用户，那么该邮件将置于管理员隔离256中。
- **管理员隔离** —当邮件符合规则下的条件时，若您希望将邮件发送至管理员隔离256中，请选择此操作。
- **重定向** —当邮件符合规则下的条件时，使用该操作，将邮件重定向至其他地址。在操作下提供了一个“*收件人*”选项，这样您便可指定将邮件重定向至哪个邮件地址。重定向的邮件将不会发送至初始收件人...邮件被重新路由至该操作中指定的地址。
- **复制** —若您希望将邮件复制到一个额外的邮件地址，请使用此选项。在操作下提供了一个“*收件人*”选项，这样您便可指定将邮件发送至哪个邮件地址。与“重定向”类似，不同之处在于在复制操作中，初始收件人以及此操作所指定的地址都将受到该邮件的副本。若您希望将一封邮件复制到多个地址，那么您可为每个地址指定一条额外的规则。
- **发送提示（警告）** —当一封邮件符合规则下条件时，若希望向某人发送一封提示或者警告邮件，请使用此操作。若选中了此操作，会向您提供选项以指定提示的*收件人*、*发件人*、*主题*以及*邮件文本*（邮件的正文）。在提示中您可使用一些宏，从而动态地包含一些特定信息。当 SecurityGateway 碰到带宏的提示文本，它会用相应的值将其取代。可使用以下宏：

  $发件人$ —以用于符合规则邮件的 SMTP MAIL From 地址来取代。例如，“sender@example.net”。

  $发件人邮箱$ —该宏仅仅是以通过 SMTP MAIL From 命令的邮件地址的邮箱部分来取代。例如，“sender@example.net”地址中的“sender”。

  $发件人域$ —该宏仅仅是以通过 SMTP MAIL From 命令的邮件地址的域部分来取代。例如，“sender@example.net”地址中的“example.net”。

  $收件人$ —以用于符合规则邮件的 SMTP RCPT To 地址来取代。例如，“recipient@example.com”..

  $收件人邮箱$ —该宏仅仅是以通过 SMTP RCPT To 命令的邮件地址的邮箱部分来取代。例如，“recipient@example.com”地址中的“recipient”。

$收件人域$—该宏仅仅是以通过 SMTP RCPT To 命令的邮件地址的域部分来取代。例如，"recipient@example.com"地址中的"example.com"。

$主题$该宏是以符合条件的邮件"主题"报头的内容来取代。

$邮件 ID$—该宏是以邮件的"邮件 ID"报头之值来取代。

$日期戳$—该宏是以邮件的日期来取代。

$当前时间$— 该宏是以 SecurityGateway 创建提示的当前时间来取代。

$HELO 名称$— 这是当 SecurityGateway 收到符合规则的邮件时，在 SMTP 会话过程中所通过的 HELO 域。

- **添加到邮件分值**—如果您希望在邮件符合规则条件时，为邮件评分添加特定数量的分数，请使用此操作。
- **发送为已注册邮件 (RMail)**—如果您希望在邮件符合规则条件时使用 RMail 的 Registered Email(注册邮件)功能中的一项或多项，请使用此操作。

  加密—果要加密邮件，请选择此选项。

  跟踪 & 证明—如果使用 RMail 的跟踪和证明功能，请选择此选项。

  电子签名—如果您希望使用 RMail 的电子签名功能进行电子签名文件，请选择此选项。

- **为 REQUIRETLS 标记邮件**—指示该邮件应使用 RequireTLS[101]。
- **发送为安全 web 邮件**—如果您希望使用 SecurityGateway 的安全通信[90] web 门户系统来发送邮件，而不是使用传统的邮件投递，请选择此操作。
- **添加报头** — 这是 AI 分类[243]规则操作，您可以使用该操作来将报头添加到匹配了规则条件的邮件中。指定报头名称，然后选择您是否希望报头值是邮件分类标签[240]的报头，还是您提供的自定义值。
- **标记主题报头** — 这是 AI 分类[243]规则操作，您可以用来将标签添加到邮件主题报头。您可以选择标签是否是邮件的分类标签[240]还是您提供的自定义值。

正则表达式

"数据泄露防护"的规则条件[187]支持"符合正则表达式"作为比较方法。正则表达式 (regexp) 是一个功能全面的系统，不仅帮助您搜索特定的文本字符，也可以搜索到文本类型。一个正则表达式的文本类型包含特殊字符的组合，成为*"元字符"*以及字母数字文本字符，或者"文字" (例如：abc，123，等等)。该类型用于匹配文本字符— 并附有匹配的结果，是成功还是失败。

SecurityGateway 的正则表达式方案使用的是 PERL 兼容性正则表达式 (PCRE)库。您可以在此获得正则表达式方案的更多信息：http://www.pcre.org/ 和 http://perldoc.perl.org/perlre.html。

如果要对正则表达式有一个全面的了解，请参阅：*掌握正则表达式，第三版* 由 O'Reilly Media, Inc.出版。

元字符

在正则表达式中，元字符是有特定功能及用途的特殊字符。在 SecurityGateway 中的正则表达式方案可允许使用下列元字符：

\ | () [] ^ $ * + ? .

元字符	描述
\	若在一元字符钱使用反斜线 (“\”)，将使元字符被处理为文字字符。若您希望正则表达式搜索其中一个用作元字符的特殊字符，这一点是有必要的。例如，要搜索 “+”您的表达式中必须包含 “\+”。
|	使用*交替*字符 (亦叫做 *“或”*或者 *“竖线”*)，当您希望字符两侧的其中一个表达式符合目标字符。正则表达式是 “abc|xyz”。搜索一个文本字符时，会出现符合条件的 “abc”或 “xyz”。
[...]	框 (“[”及 “]”)内包含的字符组就表示该组中的任意字符都可能符合所查找的文本字符。括号里字符间的破折号 (“-”)表示了字符的范围。例如，在表达式 “[a-z]”中搜索字符 “abc”将生成三个匹配项：*“a,”* *“b，”*以及 *“c*。”使用表达式 “[az]”只会生成一个匹配项：*“a*。”
^	表示字符串的开头。在目标字符串中，“abc ab a”表达式 “^a”将生成一个匹配项—目标字符串中的第一个字符。正则表达式 “^ab”也将生成一个匹配项—*目标字符串中的*第一第二个字符。
[^...]	紧跟左括号 (“[”)后的插入记号 (“^”)有不同的含义。用于将括号内剩余的字符排除在符合条件的目标字符串之外。表达式 “[^0-9]”表明目标字符不是数字。
(...)	圆括号影响了样式估计的顺序，也可作为*带标记的*表达式，用于*搜索和替换*表达式。 正则表达式的搜索结果可以暂时保存，也可用于*替换*表达式以建立新的表达式。在*替换*表达式中，您可以包含一个 “&”或者 “\0”字符，将会以正则表达式搜索过程中所找到的子字符串来替换。所以，如果*搜索*表达式 “a(bcd)e”找到了一个子字符串匹配项，那么 “123-&-123”或者 “123-\0-123”的替换*替换*表达式将以 “123-abcde-123”来替换符合条件的文本。 同样地，在替换表达式中您也可以使用特殊字符 “\1,” “\2,” “\3,”*等等* 。这些字符只会被*已标记*表达式的结果所替代，而不是整个子字符串的匹配项。紧跟反斜线的数字表明您想要引用的带标记表达式 (如果正则

	表达式中包含了不知一个带标记的表达式）。例如，如果您的*搜索*表达式是 "(123)(456)"并且您的*替换*表达式是 "a-\2-b-\1"，那么一个符合的自字符将由 "a-456-b-123"替代，而 "a-\0-b"的一个*替换*表达式将以 "a-123456-b"替代。
$	美元记号（"$"）代表字符串的结尾。在文本字符串中，"123 321 123"表达式 "3$"将生成一个匹配项—字符串中的最后一个字符。正则表达式 "123$"也将生成一个匹配项——*目标字符串中的*最后三个字符。
*	星号（"*"）量词表明星号左边的字符*在一行字符中出现的次数*必须大于等于零次。那么 "1*abc"将符合文本 "111abc"以及 "abc"。
+	与星号量词类似，"+"量词表明加号左边的字符*在一行字符中出现的次数*必须大于等于一次。那么，"1+abc"将符合文本 "111abc"而不符合文本 "abc"。
?	问号（"?"）量词表明问号左边的字符必须符合*零或*一次。那么，"1*abc"将符合文本 "abc"，并且符合 "111abc"的 "1abc"部分。
.	句号或者点（"."）元字符将符合任何其他字符。那么 ".+abc"将符合 "123456abc"，且 "a.c"将符合 "aac"，"abc"，"acc"等等。

4.6.1 医学术语

使用这些数据泄露防护[185]选项，在邮件中搜索医学术语，并根据评分标准对这些邮件采取操作。已为您预定义了近 2000 个医学术语的列表，您可以添加自定义术语，或按需删除一些术语。每个术语都被分配一个分数，并扫描邮件来查找匹配的术语，然后计算分数的总和。然后，当计算的分数大于或等于定义的阈值时，对邮件执行指定的操作。您可以选择隔离邮件，并对其使用 RMail加密服务[183]。您还能选择从医学术语搜索中排除入站和本地邮件。

配置

检查已发送的医学术语邮件
如果您希望扫描邮件中的医学术语，请选中此框。每个术语都被分配一个分数，邮件的总分将决定对该邮件采取的措施（如果有的话）。

分值大于或等于 [xx]时隔离邮件
当启用此项，并且邮件的医学术语总分达到或超过此值时，该邮件将被移至管理隔离[256]。

为分值大于或等于 [xx]的邮件使用 RMail加密服务
当启用此项，并且邮件的医学术语总分达到或超过此值时，将为该邮件使用 RMail加密服务 183 这个选项。

排除入站邮件 (收件人是本地用户，发件人不是同一域的本地用户)
当收件人是本地用户且发件人不是同一域的本地用户时，此选项将从医学术语搜索中排除这封入站邮件。

排除内部邮件 (发件人和收件人是同一域的本地用户)
当发件人和收件人都是同一域的本地用户时，此选项将从医学术语搜索中排除该邮件。

当前定义的术语

此列表包含您定义的所有医学术语及其相应的分数。当扫描邮件中的医学术语时，将任何所列术语的每次出现的分数加在一起以获得最终分数。如果分数达到或超过上面设置的指定阈值之一，则采取相关操作。

添加或编辑术语
点击 "**新建**"来将新的术语添加到列表中，或选择一个术语并点击 "**编辑**"来为该术语或其分数进行变更。定义术语及其分数后，请点击 "**保存并关闭**"。

删除术语
要从列表中删除一个或多个术语，请选择所需的术语并点击 "**删除**"。点击 "**是**"来确认您准备删除此限制的决定。

导入医学术语列表
要导入一个医学术语列表：

1. 创建一个纯文本文件，将以下内容作为第一行："Term","Score"
2. 对于之后的每一行，使用相同的格式列出一个术语及其相关分数。例如："Abacavir sulfate","10"
3. 完成后，使用扩展名 "csv"来保存文件。例如 "medical_terms.csv"。
4. 在 "医学术语"页面，请点击 "**导入**"。
5. 点击 "**关闭文件**"，请导航至您创建的文件并点击 "**打开**"。
6. 如果您想用您的自定义列表替换当前的医学术语列表，请点击 "**删除现有的术语**"。**警告：这将删除整个医学术语列表，并将其替换为您的列表。** 如果您只是想将自定义条款添加到列表中，请不要选中该框。
7. 点击 "**导入术语**"。
8. 点击 "**关闭**"。

导入医学术语列表
要导出当前定义的术语列表，请点击 "**导出**"，选择一个位置并点击 "**保存**"。

例外 - 域

当配置这些设置时，如果您在页面顶部的 *"针对域："* 下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。请为相应的域点击 *"查看/编辑"* 链接来查看或编辑其 "医学术语"设置，或点击 *"重置"* 来将该域的设置重置为默认的 "全局"值。

4.7 过滤

4.7.1 邮件内容

该页面用于管理您的邮件内容过滤规则。您可在此处创建，编辑或者删除您的规则，只需点击条目中的一个选择框，您即可快速地启用或者禁用任意规则。过滤规则可用于指定特定标准，它是 SecurityGateway 处理每封邮件时的测试标准。接着，若邮件符合一项规则，便可执行一系列的操作。您可以创建规则来查看特定报头是否存在，查看特定发件人或收件人，在报头或者邮件正文搜索特定文本，测试邮件的大小，以及很多其他操作。若一封邮件符合一条规则的测试，那么此项规则可导致邮件被拒收，删除，隔离，复制或者重定向至不同的地址，等等。

内容过滤规则列表有三栏：启用，描述及预览。启用栏里包含了一个每个条目的选择框，可以用来快速地启用/禁用规则。描述栏中包含了 *"规则名称"*，是由您在创建一条规则时所指定的。预览栏中包含了每条规则的图标，当您将指针悬停在某一规则时，将显示该规则的工具提示。工具提示中包含了真正的 Sieve 脚本 219，该脚本由内容过滤器编辑器 195 创建，用来为规则而服务。

页面顶部的工具栏包含了下列四个选项：

新建
点击 *"新建"* 来打开 "内容过滤规则编辑器 195"，用来创建一条新规则。

编辑
选中一条规则然后点击工具栏上的 *"编辑"*，在 "内容过滤规则编辑器中将其打开 195"。或者，您只需双击一条规则将其打开。

删除
要删除一条或多条规则，从列表中选中条目然后点击 *"删除"*。会跳出一个框，要求您确认是否决定删除规则。您可以使用 "Ctrl 和 Shift"键来选择多个条目。

针对域：
使用 *"针对域："* 通过下拉列表框来选择在列表中要显示哪条规则。您可显示全局规则，该规则适用于一切域，或者您可以显示特定域的规则。

内容过滤规则编辑器

内容过滤规则编辑器用于创建新规则或者编辑现有规则。要创建一条新规则，点击内容过滤规则工具栏上的 *"新建"*，然后逐一（顶部到底部）进入编辑器选项，每次只进入一个选项。完成后，点击 *"保存并关闭"* 来创建新规则。

已启用该规则
要创建一条新规则，必须勾选此框。至于现有的规则，您可以取消勾选此框将此规则禁用。在测试邮件时，SecurityGateway 不会使用已禁用的规则。该选项所对应的是 "内容过滤规则"列表上的 *"已启用"* 栏。

针对域：
使用此选项来选择该规则所适用的域。如果选择了“--全局--”，那么发送至或者来自于您 SecurityGateway 的一切域的全部邮件都将按照该规则进行测试。如果选择的是一个特定域，那么只需测试发送至或来自于该特定域的邮件。

规则名称：
在此输入规则的描述性名称。该选项对应的是“内容过滤规则”列表上的“*描述*”栏。

应用此规则，如果

所有条件都符合（与）
如果您希望只有当一封邮件满足了所有您所提供的如下测试条件后再匹配一条规则的话，请选择此选项。这是在测试条件下执行一个合乎逻辑的“与”。换句话来说，“若条件 A 是真的且条件 B 也是真的，那么就执行特定操作。”

...大约 [xx] 字符数以内
启用此项时，仅在*待比较项目*是正文时才应用，其中还包括 SecurityGateway 能够从中提取文本的附件。如果正文存在多个条件，那么所有这些条件都必须在彼此的指定接近度（之前或之后的字符数）内找到。匹配必须全部发生在同一个 mime 部分中，即邮件正文、备选正文或附件。在“AND”中包含的其他条件必须为 true，不过无需彼此接近。

符合任意条件（或）
如果您希望一封邮件满足了您所提供的如下测试条件中的任意一项后再匹配一条规则的话，请选择此选项。这是在测试条件下执行一个合乎逻辑的“或”。换句话来说，“若条件 A 是真的或者条件 B 是真的，那么就执行特定操作。”

条件：
该框显示您为规则提供的所有当前测试条件。点击框中的条件，您可以编辑任意一项。点击紧靠条件旁边的**[Remove]**，您可以删除任意一项。

添加条件
请点击“**添加条件**”来新建一个条件，以便添加到该规则当前的*条件*列表中。添加完条件后，您可通过再次点击该链接来添加更多条件。有关不同类型条件的更多信息，还请参阅下方的规则条件 196。

操作：
当一封邮件符合规则条件时，从此列表中选出您希望执行的操作。若选中操作需要更多数据，在此操作下会出现一个相应的控件让您输入该数据。欲获得您可以执行的不同类型操作的信息，请见下方的操作 199。当您为您的规则设置完所有条件并且选中了一项操作后，请点击“*保存并关闭*”来关闭编辑器并在列表中添加新规则。

规则条件

当您希望给一条规则添加一个测试条件时，您将会使用“*点击此处为该规则添加一个条件*”链接来打开规则条件这一屏幕。在使用该屏幕来创建测试条件时，您必须首先指定邮件属性，或者您欲进行测试或比较的项目。接着，您必须指定如何测试或比较此项目：该项目是否包含特定文本，它是否完全等同于特定文本，是否存在特定的报头，等等。有若干可被测试的项目，并有多种常见的测试方法。当您已选中项目、测试方法且已输入任何所需信

息，请点击 *"保存并关闭"*从而向您的规则中添加测试条件。

要比较的项目：
这些是您可以在邮件中测试的项目。

- **MAIL (From)** —该测试使用的值就是 SMTP "MAIL From"命令所通过的值。这就表明了邮件从何而来，不过并不一定要与邮件的 "发件人"报头所包含的信息完全一致。有时 "发件人"报头会包含额外信息或者不同信息。除了那九种常见的测试或比较项目的方法之外 (见下)，该项目同样可以进行比较，使用 "是本地用户"和 "非本地用户"测试。
- **RCPT (To)** — 该测试使用的值就是 SMTP "RCPT To"命令所通过的值。这就表明了邮件从何而来，不过并不一定要与邮件的 "收件人"报头所包含的信息完全一致。有时 "收件人"报头会包含额外信息或者不同信息。除了那九种常见的测试或比较项目的方法之外 (见下)，该项目同样可以进行比较，使用 "是本地用户"和 "非本地用户"测试。
- **MAIL and RCPT** —选择此项目来使用 SMTP "MAIL From"和 SMTP "RCPT To"命令来确定邮件是入站、出站还是内部邮件 (请参阅下方的 *"额外测试方法"*)。
- **IP**—选择该项目来测试发件服务器或客户端的 IP 地址。
- **HEADER** — 如果您希望指定一个要比较的报头，请选择该项目。若选中，将出现一个 *"报头名称"*选项，让您指定对于此测试条件，将使用哪个报头。除了那九种常见的测试项目的方法之外，该项目同样可以进行比较，使用 "报头存在"以及 "报头不存在"测试。**注意：**在指定 *"报头名称"*时，在报头名称里不要使用冒号。例如，使用 "发件人"作为 *"报头名称"*，而不用 "发件人："，若您希望比较发件人报头。
- **SUBJECT** —这是邮件的 "主题"报头。若您希望测试邮件的主题，请选择该项目。
- **BODY** — 选择 *"正文"*，若您希望使用邮件正文作为测试项目来比较。
- **BODY or SUBJECT** —在 *"正文"*或 *"主题"*匹配此规则条件时，如果您希望创建一个为 true 的规则，请选择此项目。这个项目是为了简化规则创建而提供的，因为它实际上等同于创建具有两个单独 "OR"语句的规则，一个搜索 *"正文"*，另一个搜索 *"主题"*来查看是否存在相同的文本。
- **ENVIRONMENT (SecurityGateway)** — 如果希望测试条件基于 SecurityGateway 的环境因素，请选择此项，例如：邮件是否来自域邮件服务器 66，发件人是否经过验证，是否位于允许列表 212或阻止列表 205，邮件分值 143是否大于或等于指定的分数，是否邮件被标记为已隔离 (用户) 255或已隔离 (管理员) 256。

如何比较：
此列表中包含了可用来测试或比较项目的方法，这些项目是在 *"上述想比较的对象"*选项里选中的。对于所有项目来说，有多种常见的测试方法。MAIL and RCPT 与 ENVIRONMENT (SecurityGateway) 项目有独特的比较程序集，Mail(From)、RCPT(To) 和 Header 有额外的测试方法。

常见的测试方法：
这些测试方法每一种都是将上述要比较的项目中选中的项目与 *您在下方所指定的如何比较中所选中方法*的搜索值相比较。这些类型的比较都对上方的 *"特比较项目"*选项可用，MAIL、RCPT 和 ENVIRONMENT (SecurityGateway) 除外。他们每个人都有一组独特的比较程序。

- **包含** — 若选中了此方法，如果 *"搜索值"*是一个子字符串或是 *上述指定的要比较*

项目的一部分，那么该比较符合条件或者是 "true"。例如，若您选择了 "MAIL (From)"作为要比较的项目，然后选择 "包含"作为比较的方法，以 "example.com"作为 *"搜索值"*，那么来自于含有 "example.com"地址的任意一封邮件都将符合该条件。

- **不包含**—若选中了此方法，如果 *"搜索值"*不是一个子字符串，也不是*上述指定的要比较项目的一部分*，那么该比较符合条件或者是 "true"。例如，若您选择了 "MAIL (From)"作为要比较的项目，然后选择 "不包含"作为比较的方法，以 "example.com"作为 *"搜索值"*，那么除了那些含有 "example.com"地址的邮件外，其他任意一封邮件都将符合该条件。
- **包含文字**—T此比较器类似于 "包含"，不过仅在字边界锚跟随在此字符串后面时才匹配。这避免了需要手动创建以下格式：\b(word1|word2|word3)\b。例如：一个规则搜索*包含* "cat"的邮件正文时，只有邮件包含完整的 "cat"时才匹配。如果邮件包含 *catfish* 或 *certificate* 则不匹配。
- **不包含文字**—T此比较器类似于 "不包含"，不过仅在不存在含有跟随在此字符串后的字边界锚的字符串时才匹配。例如：一个规则搜索*不包含* "cat"的邮件正文时，将匹配不包含完整 "cat"的任何邮件，即使正文包含 *catfish* 或 *certificate* 时也匹配。
- **等于**—此方法与上述的 *"包含"*类似，不同之处在于 *"搜索值"*必须与 *"要比较项目的值"*完全匹配，而不是仅仅是该值的一部分。例如，若您选择了 IP 作为要比较的项目，然后选择 "等于"作为比较的方法，以 "192.168.0.1"作为 *"搜索值"*，那么只有来自于该准确 IP 地址的邮件才符合条件。
- **不等于**—此类型的比较与先前的方式正好相反。如果 *"要比较项目的值"*与 *"搜索值"不完全相同*，那么该比较是真的。例如，若您选择了 IP 作为要比较的项目，然后选择 "等于"作为比较的方法，以 "192.168.0.1"作为 *"搜索值"*，那么除了那些来自于该准确 IP 地址的邮件外，其他任意一封邮件都符合条件。
- **以...开头**—当 *"搜索值"*与上述所指定的要比较项目的值开头相符时，*若您希望考虑一个条件为 True*，那么请使用此类型的比较。例如，若您选择 *"主题"*作为要比较的项目，"[allstaff]"作为搜索值，那么所有主题行以 "[allstaff]"开头的邮件都符合条件。
- **不以...开头**—与先前的比较类型正好相反。当 *"搜索值"*与上述所指定的要比较项目的值开头不相符时，*若您希望考虑一个条件为 True*，那么请使用此选项。例如，若您选择 *"主题"*作为要比较的项目，"[allstaff]"作为搜索值，那么除了主题行以 "[allstaff]"开头的邮件以外，其他任意邮件都符合条件。
- **以...结尾**—该比较指的是每当 *"要比较项目的值"*以 *"搜索值"*作为结尾，即符合了条件。例如，若您选择了 RCPT (To) 作为要比较的项目且将 "以...结尾"作为比较方法，以 ".cn"作为搜索值，那么以 ".cn"作为邮件地址结尾的全部邮件都将符合条件。
- **不以...结尾**—该比较指的是每当 *"要比较项目的值"*不以 *"搜索值"*作为结尾，即符合了条件。例如，若您选择了 RCPT (To) 作为要比较的项目且将 "以...结尾"作为比较方法，以 ".cn"作为搜索值，那么除了以 ".cn"作为邮件地址结尾的全部邮件之外，其他任意邮件都将符合条件。
- **匹配正则表达式**—如果您希望在以下情况使用正则表达式，即比较在上方 *"特比较项目"*这一选项中选定的项目，请选择此项。

额外的测试方法：

- **是本地用户**—该比较方法只适用于上述的 MAIL (From) 以及 RCPT (TO) 选

项。当邮件地址是本地的 SecurityGateway 用户时，若您希望符合条件或条件为 "true"，请选择此选项。例如，若您选择 MAIL (From) 作为 *"要比较的项目"*，那么只有来自于本地用户的邮件才符合条件。

- **非本地用户**—该比较方法只适用于上述的 MAIL (From) 以及 RCPT (TO) 选项。当邮件地址不是本地的 SecurityGateway 用户时，若您希望符合条件或条件为 "true"，请选择此选项。例如，若您选择 MAIL (From) 作为 *"要比较的项目"*，那么来自于远程用户的所有邮件都符合条件。
- **报头存在**—只有当您选择 "报头"作为 *"要比较的项目"时*，此选项才可用。当您选择了此选项并且在 *"所提供的选项中"*指定了报头的名称，只有当邮件中出现指定报头时才符合条件。例如，若您指定了 "X-我的-自定义-报头"作为 *"报头名称"*，那么所有显示该报头的邮件都符合条件。无此报头的任意一封邮件都不符合条件。
- **报头不存在**—只有当您选择 "报头"作为 *"要比较的项目"时*，此选项才可用。当您选择了此选项并且在所提供的选项中指定了 *"报头名称"*，只有当邮件中不显示指定报头时才符合条件。例如，若您指定了 "X-我的-自定义-报头"作为 *"报头名称"*，那么所有不显示该报头的邮件都符合条件。显示此报头的任意一封邮件都不符合条件。
- **邮件是/不是 [入站 | 出站 | 内部]**— 这些比较程序仅适用于MAIL and RCPT 项目。SMTP "MAIL From"和 SMTP "RCPT To"值都用于确定邮件是否为入站，出站或内部邮件。
  - **入站**—邮件是指向本地用户的，而不是来自同一个域的本地用户。
  - **出站**—邮件是来自本地用户的，而不是指向同一个域的本地用户。
  - **内部**—邮件来往于同一个域的本地用户。
- **ENVIRONMENT (SecurityGateway) 测试方式** — 以下测试方法仅适用于在您选择了 ENVIRONMENT (SecurityGateway) 作为 *"特比较项目"*的时候：
  - **域邮件服务器** — 该邮件来自或不来自您的域邮件服务器[66]。
  - **已验证发件人**— 选择此项，可根据发件人是否经过身份验证来设置条件。
  - **发件人位于 [允许列表 | 阻止列表]**— 是否是位于允许列表[212]或阻止列表[205]上的发件人。
  - **邮件分值 (大于或等于)**— 使用此项来基于邮件分值[143]设置规则。
  - **已标记邮件：[已隔离 (用户) | 已隔离 (管理员)]**— 按照邮件是否被标记为已隔离 (用户)[255]或已隔离 (管理员)[256]来设置条件。

操作

待为您的规则设置完所有条件后，使用 "规则编辑器"上的 *"操作"*选项来选择当一封邮件符合规则条件时所要执行的操作。有七种操作可供选择：

- **拒收**— 若您希望拒收一封符合该规则内条件的邮件，请选择此操作。当选中了该选项时，在操作下方会出现一个 *"SMTP 反应"*选项，您可以指定在邮件拒收时所发送的文本反应。例如，在 *"SMTP 反应"*选项中，若您使用了，"我们不需要你的垃圾邮件！"，在 SMTP 会话过程中，当 SecurityGateway 拒收一封符合规则的邮件

时，它将会发送 "550 我们不要你的垃圾邮件。"

- **删除**—当一封邮件符合规则的条件时，该操作将使邮件被删除。与 "拒收"操作不同的是，该选项不会发送 SMTP 反应，也不会发送投递失败邮件，就单纯地将邮件删除。
- **隔离**—若选中了该操作，如果收件人是本地用户，那么符合该规则下条件的邮件将置于收件人的隔离[255]中。如果收件人是远程用户，那么该邮件将置于管理员隔离[256]中。
- **管理员隔离**—当邮件符合规则下的条件时，若您希望将邮件发送至管理员隔离[256]中，请选择此操作。
- **重定向**—当邮件符合规则下的条件时，使用该操作，将邮件重定向至其他地址。在操作下提供了一个 *"收件人"*选项，这样您便可指定将邮件重定向至哪个邮件地址。重定向的邮件将不会发送至初始收件人...邮件被重新路由至该操作中指定的地址。
- **复制**—若您希望将邮件复制到一个额外的邮件地址，请使用此选项。在操作下提供了一个 *"收件人"*选项，这样您便可指定将邮件发送至哪个邮件地址。与 "重定向"类似，不同之处在于在复制操作中，初始收件人以及此操作所指定的地址都将受到该邮件的副本。若您希望将一封邮件复制到多个地址，那么您可为每个地址指定一条额外的规则。
- **发送提示 (警告)**—当一封邮件符合规则下条件时，若希望向某人发送一封提示或者警告邮件，请使用此操作。若选中了此操作，会向您提供选项以指定提示的*收件人*、*发件人*、*主题*以及*邮件文本* (邮件的正文)。在提示中您可使用一些宏，从而动态地包含一些特定信息。当 SecurityGateway 碰到带宏的提示文本，它会用相应的值将其取代。可使用以下宏：

  $发件人$—以用于符合规则邮件的 SMTP MAIL From 地址来取代。例如，"sender@example.net"。

  $发件人邮箱$—该宏仅仅是以通过 SMTP MAIL From 命令的邮件地址的邮箱部分来取代。例如，"sender@example.net"地址中的 "sender"。

  $发件人域$—该宏仅仅是以通过 SMTP MAIL From 命令的邮件地址的域部分来取代。例如，"sender@example.net"地址中的 "example.net"。

  $收件人$—以用于符合规则邮件的 SMTP RCPT To 地址来取代。例如，"recipient@example.com"..

  $收件人邮箱$—该宏仅仅是以通过 SMTP RCPT To 命令的邮件地址的邮箱部分来取代。例如，"recipient@example.com"地址中的 "recipient"。

  $收件人域$—该宏仅仅是以通过 SMTP RCPT To 命令的邮件地址的域部分来取代。例如，"recipient@example.com"地址中的 "example.com"。

  $主题$该宏是以符合条件的邮件 "主题"报头的内容来取代。

  $邮件 ID$—该宏是以邮件的 "邮件 ID"报头之值来取代。

  $日期戳$—该宏是以邮件的日期来取代。

  $当前时间$— 该宏是以 SecurityGateway 创建提示的当前时间来取代。

  $HELO 名称$— 这是当 SecurityGateway 收到符合规则的邮件时，在 SMTP 会话过程中所通过的 HELO 域。

- **添加到邮件分值**—如果您希望在邮件符合规则条件时，为邮件评分添加特定数量

的分数，请使用此操作。

- **发送为已注册邮件 (RMail)**—如果您希望在邮件符合规则条件时使用 RMail的 Registered Email(注册邮件)功能中的一项或多项，请使用此操作。

  加密—果要加密邮件，请选择此选项。

  跟踪 & 证明—如果使用 RMail的跟踪和证明功能，请选择此选项。

  电子签名—如果您希望使用 RMail的电子签名功能进行电子签名文件，请选择此选项。

- **为 REQUIRETLS 标记邮件**—指示该邮件应使用 RequireTLS[101]。
- **发送为安全 web 邮件**—如果您希望使用 SecurityGateway 的安全通信[90] web 门户系统来发送邮件，而不是使用传统的邮件投递，请选择此操作。
- **添加报头** — 这是 AI 分类[243]规则操作，您可以使用该操作来将报头添加到匹配了规则条件的邮件中。指定报头名称，然后选择您是否希望报头值是邮件分类标签[240]的报头，还是您提供的自定义值。
- **标记主题报头** — 这是 AI 分类[243]规则操作，您可以用来将标签添加到邮件主题报头。您可以选择标签是否是邮件的分类标签[240]还是您提供的自定义值。

正则表达式

内容过滤器的规则条件[196]支持"符合正则表达式"作为比较方法。正则表达式 (regexp)是一个功能全面的系统，不仅帮助您搜索特定的文本字符，也可以搜索到文本类型。一个正则表达式的文本类型包含特殊字符的组合，成为 *"元字符"*以及字母数字文本字符，或者 *"文字"* (例如：abc，123，等等)。该类型用于匹配文本字符— 并附有匹配的结果，是成功还是失败。

SecurityGateway 的正则表达式方案使用的是 PERL 兼容性正则表达式 (PCRE)库。您可以在此获得正则表达式方案的更多信息：http://www.pcre.org/ 和 http://perldoc.perl.org/perlre.html。

如果要对正则表达式有一个全面的了解，请参阅：*掌握正则表达式，第三版* 由 O'Reilly Media, Inc.出版。

元字符

在正则表达式中，元字符是有特定功能及用途的特殊字符。在 SecurityGateway 中的正则表达式方案可允许使用下列元字符：

\ | () [] ^ $ * + ? .

元字符	描述
\	若在一元字符钱使用反斜线 ("\")，将使元字符被处理为文字字符。若您希望正则表达式搜索其中一个用作元字符的特殊字符，这一点是有必要的。例如，要搜索 "+"您的表达式中必须包含 "\+"。

|	使用*交替*字符（亦叫做*"或"*或者*"竖线"*），当您希望字符两侧的其中一个表达式符合目标字符。正则表达式是"abc|xyz"。搜索一个文本字符时，会出现符合条件的"abc"或"xyz"。
[...]	框（"["及"]"）内包含的字符组就表示该组中的任意字符都可能符合所查找的文本字符。括号里字符间的破折号（"-"）表示了字符的范围。例如，在表达式"[a-z]"中搜索字符"abc"将生成三个匹配项：*"a,"*、*"b,"*以及*"c。"*使用表达式"[az]"只会生成一个匹配项：*"a。"*
^	表示字符串的开头。在目标字符串中，"abc ab a"表达式"^a"将生成一个匹配项—目标字符串中的第一个字符。正则表达式"^ab"也将生成一个匹配项—*目标字符串中的*第一第二个字符。
[^...]	紧跟左括号（"["）后的插入记号（"^"）有不同的含义。用于将括号内剩余的字符排除在符合条件的目标字符串之外。表达式"[^0-9]"表明目标字符不是数字。
(...)	圆括号影响了样式估计的顺序，也可作为*带标记的*表达式，用于*搜索和替换*表达式。 正则表达式的搜索结果可以暂时保存，也可用于*替换*表达式以建立新的表达式。在*替换*表达式中，您可以包含一个"&"或者"\0"字符，将会以正则表达式搜索过程中所找到的子字符串来替换。所以，如果*搜索*表达式"a(bcd)e"找到了一个子字符串匹配项，那么"123-&-123"或者"123-\0-123"的替换*替换*表达式将以"123-abcde-123"来替换符合条件的文本。 同样地，在替换表达式中您也可以使用特殊字符"\1,""\2,""\3,"*等等*。这些字符只会被*已标记*表达式的结果所替代，而不是整个子字符串的匹配项。紧跟反斜线的数字表明您想要引用的带标记表达式（如果正则表达式中包含了不知一个带标记的表达式）。例如，如果您的*搜索*表达式是"(123)(456)"并且您的*替换*表达式是"a-\2-b-\1"，那么一个符合的自字符将由"a-456-b-123"替代，而"a-\0-b"的一个*替换*表达式将以"a-123456-b"替代。
$	美元记号（"$"）代表字符串的结尾。在文本字符串中，"13 321 123"表达式"3$"将生成一个匹配项—字符串中的最后一个字符。正则表达式"123$"也将生成一个匹配项——*目标字符串中的*最后三个字符。
*	星号（"*"）量词表明星号左边的字符*在一行字符中出现的次数*必须大于等于零次。那么"1*abc"将符合文本"111abc"以及"abc"。

+	与星号量词类似，“+”量词表明加号左边的字符*在一行字符中出现的次数*必须大于等于一次。那么，“1+abc”将符合文本“111abc”而不符合文本“abc”。
?	问号（“?”）量词表明问号左边的字符必须符合*零或*一次。那么，“1*abc”将符合文本“abc”，并且符合“111abc”的“1abc”部分。
.	句号或者点（“.”）元字符将符合任何其他字符。那么“.+abc”将符合“123456abc”，且“a.c”将符合“aac”，“abc”，“acc”等等。

4.7.2 附件

您可使用该页面上的选项来指定特定的文件格式，每当附上此类文件中的其中一种，便会造成邮件被阻止或隔离。您可全局定义过滤限制，也可逐域定义。

要阻止的附件

在该部分指定您想要阻止的文件类型。如果邮件中附上了其中的一种文件类型，那么在 SMTP 进程中该邮件将被阻止。

如果您同时在阻止和隔离部分列出了相同的文件类型，那么包含该类型附件的邮件将被**阻止**，而不是被隔离。

添加
要在阻止列表中添加一个新的文件类型，请在此输入然后点击*“添加”*。

删除
要从阻止列表中删除一个文件类型，请从列表中选中该文件并点击*“删除”*。在选中文件时按住 CTRL 键，您即可选中多个文件。

建议
这些链接提供了更快捷的方式来添加常见文件类型至阻止列表。只需点击一个链接即可将这些文件类型添加到该列表。**请注意：**将打开一个确认框，列出如果您希望继续，将被阻止的所有特定文件类型。

阻止建议的文件（默认）：
点击此链接，可将默认推荐的文件类型添加到阻止列表中。当您更新了 SecurityGateway，并希望确保阻止最新的推荐文件类型时，这将非常有用。

阻止可执行的文件：
该链接将 APP、CMD、COM、DMG、EXE、HTA、PIF、SCR 以及 VBS 类型的文件添加至阻止列表。

阻止图像文件：
点击该链接，添加下列图像文件类型至阻止列表：BMP、GIF、JPG、PNG、TIF 以及 TIFF。

阻止视频文件：
点击该链接从而阻止以下视频文件类型：3GP、ASX、AVI、DIVX、M4U、MOV、MP4、MPEG、MPG、QT、RM、RTS、SWF、WM 以及 WMV。

阻止音频文件：
该链接阻止了以下音频文件类型：AAC、AIF、AIFF、AU、CDR、M3U、M4A、MID、MIDI、MOD、MP3、OGG、RA、WAV 以及 WAVE。

阻止压缩文件：
该链接将以下文件压缩类型添加至阻止列表：GZ、GZIP、RAR、TAR、TAR、GZ、TGZ 以及 ZIP。

排除发送到下列电子邮件地址的邮件
选中此框，并添加您希望从 "要阻止的附件"选项中排除的任何收件人地址。允许使用电子邮件地址掩码。示例：*@company.mail、user*@company.mail、admin@*.mail

要隔离的附件

在该部分指定您想要隔离的文件类型。当一封邮件的附件中包含了这些文件类型的其中一种，该邮件将先接收然后隔离。

如果您同时在阻止和隔离部分列出了相同的文件类型，那么包含该类型附件的邮件将被**阻止**，而不是被隔离。

添加
要在隔离列表中添加一个新的文件类型，请在此输入然后点击 *"添加"*。

删除
要从隔离列表中删除一个文件类型，请从列表中选中该文件并点击 *"删除"*。在选中文件时按住 CTRL 键，您即可选中多个文件。

建议
这些链接提供了更快捷的方式来添加常见文件类型至隔离列表。只需点击一个链接，即可添加那些类型的文件。

隔离可执行的文件：
该链接将 APP、CMD、COM、DMG、EXE、HTA、PIF、SCR 以及 VBS 类型的文件添加至隔离列表。

隔离图像文件：
点击该链接，添加下列图像文件类型至隔离列表：BMP、GIF、JPG、PNG、TIF 以及 TIFF。

隔离视频文件：
点击该链接隔离以下视频文件类型：3GP、ASX、AVI、DIVX、M4U、MOV、MP4、MPEG、MPG、QT、RM、RTS、SWF、WM 以及 WMV。

隔离音频文件：
该链接隔离以下音频文件类型：AAC、AIF、AIFF、AU、CDR、M3U、M4A、MID、MIDI、MOD、MP3、OGG、RA、WAV 以及 WAVE。

隔离压缩文件：
该链接将以下文件压缩类型添加至隔离列表：GZ、GZIP、RAR、TAR、TAR、GZ、TGZ 以及 ZIP。

排除发送到下列电子邮件地址的邮件
选中此框，并添加您希望从 "要隔离的附件"选项中排除的任何收件人地址。允许使用电子邮件地址掩码。示例：*@company.mail、user*@company.mail、admin@*.mail

例外 - 域

当配置这些设置时，如果您在页面顶部的 *"针对域："* 下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。为相应域点击 *"查看/编辑"* 链接来查看或编辑其过滤设置，或者点击 *"重置"*，将域设置重置为默认的全局值。

4.8 阻止名单

阻止列表是一些列表，如果您希望阻止或者隔离某些邮件，会于此列出其邮件地址，主机与 IP 地址。根据默认这些邮件在 SMTP 会话过程中将被拒收，但是在 阻止列表操作 211 页面您可改变此设置，以隔离的方式取而代之。此项操作可通过全局设置，也可为特定的域设置，而且阻止列表本身也可设为全局或者是特定域。此外，虽然每次加入阻止列表的项目只有一个，不过每一个阻止列表都有其导入功能，这便允许您使用逗号分隔的文件立刻添加多个项目。最后，每一项列表都有一个导出功能，让您能够将阻止列表的内容保存为一个 CSV 文件。有三种类型的阻止列表，它们皆可全局设置，也可为指定域设置：

地址阻止列表 205 — 使用该阻止列表来阻止或隔离来自于特定邮件地址的邮件。

主机阻止列表 207 — 此阻止列表是基于投递邮件的特定主机来阻止或隔离邮件 例如：mail.example.com，smtp.example.net 等等）。

IP 阻止列表 209 — IP 阻止列表是基于试图发送邮件的主机的 IP 地址来阻止或隔离邮件。

4.8.1 地址

使用该阻止列表来阻止或隔离来自于特定邮件地址的邮件。根据默认这些邮件在 SMTP 会话过程中将被拒收，但是在 阻止列表操作 211 页面您可改变此设置，以隔离的方式取而代之。此项操作可通过全局设置，也可为特定的域设置，而且地址阻止列表本身也可设为全局或者是特定域。此外，虽然每次加入阻止列表的项目只有一个，不过每一个黑名单都

有其导入功能，这便允许您使用逗号分隔的文件立刻添加多个项目。最后，它还有一个导出功能，让您能够将阻止列表的内容保存为一个 CSV 文件。

添加地址到阻止列表

要添加一个地址到地址阻止列表，请点击页面顶部工具栏上的 *"新建"*。这将打开阻止列表条目 207 页面，以添加地址 (见下)。

编辑被列入阻止列表的地址

要编辑一条列于阻止列表的地址，请双击您希望编辑的条目，或选中要编辑的条目并单击位于该页顶部工具栏中的*编辑*。这将会在阻止列表条目 207 页面打开该条目。

删除被列入阻止列表的地址

要删除一条或多条列于阻止列表的地址，选中要删除的条目并单击位于该页顶部工具栏中的 *"删除"*。在点击每个条目的同时按下 CTRL 键可选择多个条目。点击 *"删除"*后，会弹出确认框，询问您是否确实要删除选定项。

导入地址到阻止列表

要导入一地址列表到地址阻止列表，请点击页面顶部工具栏上的 *"导入"*。这会打开导入列表页。使用该页上的 *"浏览"*按钮找到包含要导入地址的 CSV 文件，然后点击 *"导入列表"*。

CSV 文件格式

您可以使用任意文本编辑器，例如记事本，来创建为添加地址到阻止列表而准备的 CSV 文件。只需按以下格式创建文件并保存为*文件名.csv*。每个 CSV 文件的第一行必须是映射行，以使服务器了解数据的排列顺序。文件中的每一项都必须包含在引号中，并以逗号分隔。

将地址导入全局阻止列表：
"*值*"栏是用于您想要列入阻止列表的邮件地址， *"类型"*栏应该说成"BlockListAddressGlobal","*注释*"栏是用于对于每一条目，您可能想加上自己的引用。*"注释"*列是可选的，但若包含了注释列，则不含注释的任意条目都需使用空白引号。

CSV 文件示例：

```
"Value","Type","Comments"
"address01@example.net"、"BlockListAddressGlobal"、"这是关于地址的注释。"
"address01@example.org","BlockListAddressGlobal",""
"address02@example.net","BlockListAddressGlobal"、"这是另一个注释。"
```

将地址导入一个特定域的邮件阻止列表：
*域*栏就是用于该阻止列表所属之域。例如，如果您想要将地址添加至 example.com 的阻止列表，那么请使用 "域"栏中的*"example.com"* 。*值*栏是用于您想要列入阻止列表的邮件地址， *类型* 栏应该说，"BlockListAddressDomain",以及 *注释* 栏是用于对于每一条目，您可能想加上自己的引用。*"注释"*列是可选的，但若包含了注释列，则不含注释的任意条目都需使用空白引号。

CSV 文件示例：

```
"Domain","Value","Type","Comments"
"example.com"、"address01@example.net"、"BlockListAddressDomain"、"这是关于地址的注释。"
```

"example.com"、"address01@example.org"、"BlockListAddressDomain"、""
"example.com"、"address02@example.net"、"BlockListAddressDomain"，"这是另一条注释。"

从阻止列表导出地址

要导出一个地址阻止列表：

1. 在*针对域：*下拉列表框中，选择全局或特定域。
2. 在页面顶部工具栏上点击 *"导出"*。这会打开文件下载对话框。
3. 点击 *"保存"*。
4. 选择文件名称和位置。
5. 点击 *"保存"*，然后是 *"关闭"*。

阻止列表条目

该页面用来向阻止列表添加新地址以及编辑现有的条目。每当您点击地址阻止列表中的*新建*或者*编辑*，便会将其打开。

列表项

针对域：
使用该下拉列表框来添加地址到指定域的阻止列表，或者如果您想要添加地址到全局列表中，请选择全局。

电子邮件地址：
在此处输入邮件地址，您想要阻止或隔离谁的邮件。在阻止列表操作 211 页面上的设置决定了邮件是否要被阻止或隔离。您可以在地址的邮箱部分使用星号，以将该域的所有地址归入阻止列表。例如，"*@example.org"将会阻止或隔离所有来自于 example.org 的邮件。

注释：
在该区域可输入有关该条目的任意注释或说明，供自己参考。

保存与关闭
当您完成对条目的添加或编辑，请点击 *"保存并关闭"*以向阻止列表保存该条目。

关闭
如果您希望关闭阻止列表条目页面同时不作任何保存，请单击该按钮。

4.8.2 主机

用此阻止列表来阻止或隔离由特定主机投递的邮件（例如，"mail.example.com"）。根据默认这些邮件在 SMTP 会话过程中将被拒收，但是在 阻止列表操作 211 页面您可改变此设置，以隔离的方式取而代之。此项操作可通过全局设置，也可为特定的域设置，而且 "主机阻止列表"本身也可设为全局或者是特定域。此外，虽然每

次加入阻止列表的项目只有一个，不过每一个黑名单都有其导入功能，这便允许您使用逗号分隔的文件立刻添加多个项目。最后，它还有一个导出功能，让您能够将阻止列表的内容保存为一个 CSV 文件。

将主机加入阻止列表

要添加一个主机到主机阻止列表，请点击页面顶部工具栏上的 *"新建"*。将会打开 阻止列表条目 209 页面来添加主机 (见下)。

编辑被列入阻止列表的主机

要编辑其中一个已列入阻止列表的主机，请双击您想要编辑的条目，或者选中想要的条目后单击 *页面顶部工具栏上的* 编辑。这将会在阻止列表条目 209 页面打开该条目。

删除被列入阻止列表的主机

要删除一个或多个已列入阻止列表的主机，请选中想要的条目然后单击 *页面顶部工具栏上的* 删除。在点击每个条目的同时按下 CTRL 键可选择多个条目。点击 *"删除"*后，会弹出确认框，询问您是否确实要删除选定项。

将主机导入阻止列表

要将主机列表导入到主机阻止列表，请点击页面顶部工具栏上的 *"导入"*。这会打开导入列表页。使用该页上的 *"浏览"*按钮找到包含要导入主机的 CSV 文件，然后点击 *"导入列表"*。

CSV 文件格式

您可以使用任意文本编辑器，例如记事本，来创建为添加主机到阻止列表而准备的 CSV 文件。只需按以下格式创建文件并保存为*文件名.csv*。每个 CSV 文件的第一行必须是映射行，以使服务器了解数据的排列顺序。文件中的每一项都必须包含在引号中，并以逗号分隔。

将主机导入全局阻止列表：

"*值*"栏是用于您想要列入阻止列表的主机，*类型* 栏应该说，"BlockListHostGlobal"，以及*注释* 栏是用于对于每一条目，您可能想加上自己的引用。*"注释"*列是可选的，但若包含了注释列，则不含注释的任意条目都需使用空白引号。

CSV 文件示例：

```
"Value","Type","Comments"
"example.net"、"BlockListHostGlobal"、"这是关于地址的注释。"
"mail.domain.com"、"BlockListHostGlobal"、""
"smtp.company.mail"、"BlockListHostGlobal"、"这是另一个注释。"
```

将主机导入一个特定域的邮件阻止列表：

*域*栏就是用于该阻止列表所属之域。例如，如果您想要将地址添加至 example.com 的主机阻止列表，那么请使用 域栏中的*"example.com"*。*值*栏是用于您想要列入阻止列表的主机 (例如：mail.example.com、domain.com 等等)，*类型* 栏应该说，"BlockListHostDomain"，以及 *注释* 栏是用于对于每一条目，您可能想加上自己的引用。*"注释"*列是可选的，但若包含了注释列，则不含注释的任意条目都需使用空白引号。

CSV 文件示例：

```
"Domain","Value","Type","Comments"
```

"example.com"、"example.net"、"BlockListHostDomain“、”这是关于地址的注释。”
"example.com"、"mail.domain.com"、"BlockListHostDomain"、""
"example.com"、"smtp.company.mail"、"BlockListHostDomain”、“这是另一个注释。”

从阻止列表导出主机

要导出主机阻止列表：

1. 在*针对域：*下拉列表框中，选择全局或特定域。
2. 在页面顶部工具栏上点击*“导出”*。这会打开文件下载对话框。
3. 点击*“保存”*。
4. 选择文件名称和位置。
5. 点击*“保存”*，然后是*“关闭”*。

阻止列表条目

该页面用于添加新的主机到阻止列表，以及编辑现有条目。每当您点击主机阻止列表中的*新建*或者*编辑*，便会将其打开。

列表项

针对域：
使用该下拉列表框来添加主机到指定域的阻止列表，或者若您想要添加主机到全局列表中，请选择全局。

主机：
在此处输入主机，您想要阻止或隔离谁的邮件。在阻止列表操作 211 页面上的设置决定了邮件是否要被阻止或隔离。如果您希望将一个特定域的所有主机列入阻止列表，您可以在主机名上使用一个星号。例如，“*.example.org”将会阻止或隔离所有来自于任意 example.org 的子域中的邮件，例如 mail.example.org、smtp.example.org，等等。

注释：
在该区域可输入有关该条目的任意注释或说明，供自己参考。

保存与关闭
当您完成对条目的添加或编辑，请点击*“保存并关闭”*以向阻止列表保存该条目。

关闭
如果您希望关闭阻止列表条目页面同时不作任何保存，请单击该按钮。

4.8.3 IP

用此阻止列表来阻止或隔离由特定 IP 地址投递的邮件（例如，“1.2.3.4"，"192.168.0.1”，等等）。根据默认这些邮件在 SMTP 会话过程中将被拒收，但是在 阻止列表操作 211 页面您可改变此设置，以隔离的方式取而代之。此项操作可通过

全局设置，也可为特定的域设置，而且 IP 阻止列表本身也可设为全局或者是特定域。此外，虽然每次加入阻止列表的项目只有一个，不过每一个黑名单都有其导入功能，这便允许您使用逗号分隔的文件立刻添加多个项目。最后，它还有一个导出功能，让您能够将阻止列表的内容保存为一个 CSV 文件。

添加 IP 到阻止列表

要添加一个 IP 地址到 IP 阻止列表，请点击页面顶部工具栏上的 *"新建"*。将会打开阻止列表条目 211 页面来添加 IP 地址 (见下)。

编辑被列入阻止列表的 IP 地址

要编辑其中一个已列入阻止列表的 IP 地址，请双击您想要编辑的条目，或者选中想要的条目后单击 *页面顶部工具栏上的* 编辑。这将会在阻止列表条目 211 页面打开该条目。

删除一个已列入阻止列表的 IP 地址

要删除一个或多个已列入阻止列表的 IP 地址，请选中想要的条目然后单击 *页面顶部工具栏上的* 删除"。在点击每个条目的同时按下 CTRL 键可选择多个条目。点击 *"删除"*后，会弹出确认框，询问您是否确实要删除选定项。

导入 IP 地址到阻止列表

要导入一 IP 地址列表到 IP 阻止列表，请点击页面顶部工具栏上的 *"导入"*。这会打开导入列表页。使用该页上的 *"浏览"*按钮找到包含要导入 IP 地址的 CSV 文件，然后点击 *"导入列表"*。

CSV 文件格式

您可以使用任意文本编辑器，例如记事本，来创建为添加 IP 地址到阻止列表而准备的 CSV 文件。只需按以下格式创建文件并保存为 *文件名.csv*。每个 CSV 文件的第一行必须是映射行，以使服务器了解数据的排列顺序。文件中的每一项都必须包含在引号中，并以逗号分隔。

将 IP 地址导入全局阻止列表：

"*值*"栏是用于您想要列入阻止列表的 IP 地址 CIDR 记数法和*, ? 和 *, ?, # 等通配符均支持)，*类型* 栏应该说，"BlockListIPGlobal"，以及 *注释* 栏是用于对于每一条目，您可能想加上自己的引用。*"注释"*列是可选的，但若包含了注释列，则不含注释的任意条目都需使用空白引号。

CSV 文件示例：

```
"Value","Type","Comments"
"1.2.3.4"、"BlockListIPGlobal"、"这是关于地址的注释。"
"1.1.1.1"、"BlockListIPGlobal"、""
"192.168.*.*"、"BlockListIPGlobal"、"这是另一个注释。"
```

将 IP 地址导入一个特定域的 IP 阻止列表：

*域*栏就是用于该阻止列表所属之域。例如，如果您想要将地址添加至 example.com 的 IP 阻止列表，那么请使用 域栏中的"example.com"。*值*栏是用于您想要列入阻止列表的 IP 地址 CIDR 记数法和*, ? 和 *, ?, # 等通配符均支持)，*类型* 栏应该说，"BlockListIPDomain"，以及 *注释* 栏是用于对于每一条目，您可能想加上自己的引用。*"注释"*列是可选的，但若包含了注释列，则不含注释的任意条目都需使用空白引号。

CSV 文件示例：

```
"Domain","Value","Type","Comments"
"example.com"、1.2.3.4"、"BlockListIPDomain”、“这是有关该地址的注释。“
"example.com"、"1.1.1.1"、"BlockListIPDomain"、""
"example.com"、"192.168.*.*"、"BlockListIPDomain″、″这是另一个注释。″
```

从阻止列表导出 IP 地址

要导出一个 IP 阻止列表：

1. 在*针对域：*下拉列表框中，选择全局或特定域。
2. 在页面顶部工具栏上点击*“导出”*。这会打开文件下载对话框。
3. 点击*“保存”*。
4. 选择文件名称和位置。
5. 点击*“保存”*，然后是*“关闭”*。

阻止列表条目

该页面用于添加新的 IP 地址到阻止列表，以及编辑现有条目。每当您点击 IP 阻止列表中的*“新建”*或者*“编辑”*，便会将其打开。

列表项

针对域：
使用该下拉列表框来添加地址到指定域的阻止列表，或者若您想要添加地址到全局列表中，请选择全局。

IP 地址：
在此处输入 IP 邮件地址，您想要阻止或隔离谁的邮件。在阻止列表操作 211 页面上的设置决定了邮件是否要被阻止或隔离。支持 CIDR 表示法，也可使用通配符：*，?，以及 # 通过单一的条目将地址块列入阻止列表。

注释：
在该区域可输入有关该条目的任意注释或说明，供自己参考。

保存与关闭
当您完成对条目的添加或编辑，请点击*“保存并关闭”*以向阻止列表保存该条目。

关闭
如果您希望关闭阻止列表条目页面同时不作任何保存，请单击该按钮。

4.8.4 配置

当一封邮件符合任何的 SecurityGateway 阻止列表 205 的要求，那么所要执行的操作将由该页面上的设置决定。根据默认在 SMTP 会话过程中会拒收邮件，但是您可以更改设置，以隔离的方式取而代之。该操作可设置为全局，也可为指定域设置。要为一个指定域配置该设置，请从页面顶部下拉清单选择框中的*对于域：*中选择您的设置，然后点击*“保存”*。

配置

允许列表匹配优先于阻止列表匹配
如果您希望在邮件同时匹配允许列表和阻止列表时，让允许列表[212]匹配享有优先权，请勾选此框。默认情况下禁用此项，这意味着如果邮件同时匹配允许列表和阻止列表，则会将优先级赋予阻止列表。在这种情况下，取决于您所配置的下方这个*"如果邮件匹配阻止列表"*设置，将拒收或隔离邮件。

如果邮件匹配阻止列表：
当一封入站邮件来自于一名已列入阻止列表的发件人，那么将执行此此操作。

...拒收该邮件
如果选择了此选项，那么在 SMTP 会话过程中，将会拒收已列入阻止列表发件人的邮件。默认情况下，选中该选项。

与发件服务器连接断开
根据默认，在拒收邮件时，将允许 SMTP 会话正常地继续下去。如果您希望会话立即终止，可点击此选择框。在拒收邮件后，SecurityGateway 会立刻与发件服务器断开连接。

...隔离邮件
如果您希望隔离来自于已列入阻止列表的发件人的邮件而不是拒收邮件，轻选择该选项。

例外 - 域

当配置这些设置时，如果您在页面顶部的*"针对域："*下拉列表框中选择了特定域，保存设置后，该域将罗列在此处。点击*"查看/编辑"*相应域的链接来查看或编辑其"阻止列表操作"设置，或者点击*重置*，将域设置重置为默认的全局值。

4.9 允许列表

允许列表是邮件地址、主机和 IP 地址的列表，其邮件将不受多种安全限制的约束。启发式和贝叶斯[129]、DNSBL[134]、DKIM 验证[154]以及 SecurityGateway 中的所有其他安全[124]功能几乎都有选项可豁免出现在相应允许列表上的发件人、主机、邮件等等。每个允许列表都可设置为针对全局或针对域，此外，尽管在允许列表中通常一次只添加一项，但每个允许列表都有导入功能，可让您使用逗号分隔值 (CSV)文件同时添加多个项目。最后，每一项列表都有一个导出功能，让您能够将允许列表的内容保存为一个 CSV 文件。有三种类型的允许列表，它们皆可全局设置，也可为指定域设置：

地址允许列表[213] - 使用该允许列表豁免来自特定邮件地址的邮件。

主机允许列表[215] - 该允许列表用于使特定主机免受指定安全限制的约束，并基于发送邮件的特定主机 (如 mail.example.com、smtp.example.net 等)豁免邮件。

IP 允许列表[217] - IP 允许列表使特定 IP 地址免受指定安全限制的约束，并基于试图发送邮件的主机 IP 地址豁免邮件。

4.9.1 地址

地址允许列表是发件人邮件地址的列表，其邮件将不受多种安全限制的约束。启发式和贝叶斯[129]、DNSBL[134]和 SecurityGateway 中的许多其他安全[124]功能都有选项以基于发件人的邮件地址豁免邮件。您可针对全局和针对特定域向该允许列表中添加地址，此外，尽管通常一次只添加一个地址，但另有导入功能，可让您使用逗号分隔值 (CSV)文件同时添加多个地址。最后，地址允许列表还有导出功能，可让您将允许列表内容保存为 CSV 文件。

添加地址到允许列表

要向地址允许列表中添加地址，请在页面顶部工具栏上单击*新建*。这会打开允许列表条目[214]页面用以添加地址 (如下)。

编辑允许列表地址

要编辑列入允许列表的地址，请双击想编辑的条目，或选择所需条目，然后在页面顶部工具栏上点击 *"编辑"*。这将会在允许列表条目[214]页面打开该条目。

删除列入允许列表的地址

要删除一条或多条列入允许列表的地址，请选择所需条目，然后在页面顶部工具栏上点击 *"删除"*。在点击每个条目的同时按下 CTRL 键可选择多个条目。点击 *"删除"*后，会弹出确认框，询问您是否确实要删除选定项。

将地址导入允许列表

要将地址列表导入地址允许列表，请在页面顶部工具栏上单击*导入*。这会打开导入列表页。使用该页上的 *"浏览"*按钮找到包含要导入地址的 CSV 文件，然后点击 *"导入列表"*。

CSV 文件格式

您可以使用任意文本编辑器，例如记事本，来创建为添加地址到允许列表而准备的 CSV 文件。只需按以下格式创建文件并保存为*文件名.csv*。每个 CSV 文件的第一行必须是映射行，以使服务器了解数据的排列顺序。文件中的每一项都必须包含在引号中，并以逗号分隔。

将地址导入全局允许列表：
"*值*"栏是用于您想要列入允许列表的邮件地址，*"类型"*栏应该说成"AllowListAddressGlobal"，"*注释*"栏是用于对于每一条目，您可能想加上自己的引用。*"注释"*列是可选的，但若包含了注释列，则不含注释的任意条目都需使用空白引号。

CSV 文件示例：

```
"Value","Type","Comments"
"address01@example.net","AllowListAddressGlobal","这是有关该地址的注释。"
"address01@example.org","AllowListAddressGlobal",""
"address02@example.net","AllowListAddressGlobal","这是另一个注释。"
```

将地址导入一个特定域的地址允许列表：
"*域*"栏就是用于该允许列表所属之域。例如，如果您想添加地址到 example.com 的允许列表，则在域列中使用 *"example.com"*。*值 (Value)*列是要加入允许列表的邮件地址，*类*

*型 (Type)*列应为 "AllowListAddressDomain"，而*注释 (Comments)*列是您可能想添加的与该条目有关的任何说明，供自己参考。*"注释"*列是可选的，但若包含了注释列，则不含注释的任意条目都需使用空白引号。

CSV 文件示例：

```
"Domain","Value","Type","Comments"
"example.com","address01@example.net","AllowListAddressDomain","这是有关该地址的注释。"
"example.com","address01@example.org","AllowListAddressDomain",""
"example.com","address02@example.net","AllowListAddressDomain","这是另一个注释。"
```

从允许列表导出地址

要导出一个地址允许列表：

1. 在*针对域：*下拉列表框中，选择全局或特定域。
2. 在页面顶部工具栏上点击*"导出"*。这会打开文件下载对话框。
3. 点击*"保存"*。
4. 选择文件名称和位置。
5. 点击*"保存"*，然后是*"关闭"*。

允许列表条目

该页用于向允许列表中添加新地址和编辑现有条目。每当您点击地址允许列表中的*新建*或者*编辑*，便会将其打开。

列表项

针对域：
使用该下拉列表框来添加地址到指定域的允许列表，或者若您想要添加地址到全局列表中，请选择全局。

电子邮件地址：
在此输入电子邮件地址，其邮件将不受任何安全功能的约束 (这些安全功能已设置为豁免"允许列表中所列发件人")。您可以在地址的邮箱部分使用星号，以将该域的所有地址归入允许列表。例如，"*@example.org"把来自 example.org 的所有邮件列入允许列表。

注释：
在该区域可输入有关该条目的任意注释或说明，供自己参考。

保存与关闭
完成条目编辑后，点击*"保存并关闭"*将该条目保存到允许列表中。

关闭
如果您希望关闭"允许列表条目"页面且不作保存，请点击该按钮。

4.9.2 主机

使用主机允许列表使特定主机（例如 "mail.example.com"）免受多项安全限制的约束。启发式和贝叶斯[129]、DNSBL[134] 和 SecurityGateway 中的许多其他安全[124]功能都有选项，可豁免列入允许列表的主机，或豁免由这些主机投递的邮件。您既可针对全局和又可针对特定域向该允许列表中添加主机，此外，尽管通常一次只添加一个主机，但另有导入功能，可让您使用逗号分隔值（CSV）文件同时添加多个主机。最后，主机允许列表还有导出功能，可让您将允许列表内容保存为 CSV 文件。

添加主机到允许列表

要添加一个主机到主机允许列表，请点击页面顶部工具栏上的 *"新建"*。这会打开允许列表条目[216]页面用以添加主机（如下）。

编辑允许列表主机

要编辑列入允许列表的主机，请双击想编辑的条目，或选择所需条目，然后在页面顶部工具栏上点击 *"编辑"*。这将会在允许列表条目[216]页面打开该条目。

删除允许列表主机

要删除一条或多条列入允许列表的主机，请选择所需条目，然后在页面顶部工具栏上点击 *"删除"*。在点击每个条目的同时按下 CTRL 键可选择多个条目。点击 *"删除"*后，会弹出确认框，询问您是否确实要删除选定项。

将主机导入允许列表

要导入主机列表到主机允许列表，请点击页面顶部工具栏上的 *"导入"*。这会打开导入列表页。使用该页上的 *"浏览"*按钮找到包含要导入主机的 CSV 文件，然后点击 *"导入列表"*。

CSV 文件格式

您可以使用任意文本编辑器，例如记事本，来创建为添加主机到允许列表而准备的 CSV 文件。只需按以下格式创建文件并保存为*文件名.csv*。每个 CSV 文件的第一行必须是映射行，以使服务器了解数据的排列顺序。文件中的每一项都必须包含在引号中，并以逗号分隔。

将主机导入全局允许列表：

"*值*"栏是用于您想要列入允许列表的主机，*类型* 栏应该说，"AllowListHostGlobal"，以及*注释* 栏是用于对于每一条目，您可能想加上自己的引用。*"注释"*列是可选的，但若包含了注释列，则不含注释的任意条目都需使用空白引号。

CSV 文件示例：

```
"Value","Type","Comments"
"example.net"、"AllowListHostGlobal"、"这是关于地址的注释。"
"mail.domain.com","AllowListHostGlobal",""
"smtp.company.mail"、"AllowListHostGlobal"、"这是另一个注释。"
```

将主机导入一个特定域的主机允许列表：

"*域*"栏就是用于该允许列表所属之域。例如，若想添加主机到 example.com 的主机允许列表，则在*域*列中使用 "example.com"。*值 (Value)*列是要加入允许列表的主机（例如 mail.example.com、domain.com 等），*类型 (Type)*列应为 "AllowListHostDomain"，而

*注释 (Comments)*列是您可能想添加的与该条目有关的任何说明，供自己参考。*"注释"*列是可选的，但若包含了注释列，则不含注释的任意条目都需使用空白引号。

CSV 文件示例：

```
"Domain","Value","Type","Comments"
"example.com"、"example.net"、"AllowListHostDomain"、"这是关于地址的注释。"
"example.com","mail.domain.com","AllowListHostDomain",""
"example.com"、"smtp.company.mail"、"AllowListHostDomain"、"这是另一个注释。"
```

从允许列表导出主机

要导出主机允许列表：

1. 在*针对域：*下拉列表框中，选择全局或特定域。
2. 在页面顶部工具栏上点击*"导出"*。这会打开文件下载对话框。
3. 点击*"保存"*。
4. 选择文件名称和位置。
5. 点击*"保存"*，然后是*"关闭"*。

允许列表条目

该页用于向允许列表中添加新主机和编辑现有条目。每当您点击主机允许列表中的*新建*或者*编辑*，便会将其打开。

列表项

针对域：
使用该下拉列表框来添加主机到指定域的允许列表，或者若您想要添加主机到全局列表中，请选择全局。

主机：
在此输入主机，其邮件将不受任何安全功能的约束（这些安全功能已设置为豁免"允许列表中所列发件人"或"允许列表中所列主机"）。如果您希望将特定域的所有主机列入允许列表，可在主机名中使用星号。例如，"*.example.org"将把所有来自 example.org 的子域（如 mail.example.org、smtp.example.org 等）的邮件列入允许列表。

注释：
在该区域可输入有关该条目的任意注释或说明，供自己参考。

保存与关闭
完成条目编辑后，点击*"保存并关闭"*将该条目保存到允许列表中。

关闭
如果您希望关闭"允许列表条目"页面且不作保存，请点击该按钮。

4.9.3 IP

使用 IP 允许列表使特定 IP 地址 (IPs)免受多项安全限制的约束。启发式和贝叶斯[129]、DNSBL[134]、DKIM 验证[154]和 SecurityGateway 中许多其他安全[124]功能都有选项，可豁免列入允许列表的 IP 地址，或豁免由这些 IP 地址投递的邮件。您可针对全局和针对特定域向该允许列表中添加 IP 地址，此外，尽管通常一次只添加一条 IP 地址，但另有导入功能，可让您使用逗号分隔值 (CSV)文件同时添加多个 IP 地址。最后，IP 允许列表还有导出功能，可让您将允许列表内容保存为 CSV 文件。

向允许列表中添加 IP

要向 IP 允许列表中添加 IP 地址，请在页面顶部工具栏上单击*新建*。这会打开允许列表条目[218]页面用以添加地址 (如下)。

编辑允许列表 IP 地址

要编辑列入允许列表的 IP，请双击想编辑的条目，或选择所需条目，然后在页面顶部工具栏上点击 *"编辑"*。这将会在允许列表条目[218]页面打开该条目。

删除允许列表 IP 地址

要删除一条或多条列入允许列表的地址，请选择所需条目，然后在页面顶部工具栏上点击 *"删除"*。在点击每个条目的同时按下 CTRL 键可选择多个条目。点击 *"删除"*后，会弹出确认框，询问您是否确实要删除选定项。

将 IP 地址导入允许列表

要将 IP 地址列表导入 IP 允许列表，请在页面顶部工具栏上单击*导入*。这会打开导入列表页。使用该页上的 *"浏览"*按钮找到包含要导入 IP 地址的 CSV 文件，然后点击 *"导入列表"*。

CSV 文件格式

您可以使用任意文本编辑器，例如记事本，来创建为添加 IP 地址到允许列表而准备的 CSV 文件。只需按以下格式创建文件并保存为*文件名.csv*。每个 CSV 文件的第一行必须是映射行，以使服务器了解数据的排列顺序。文件中的每一项都必须包含在引号中，并以逗号分隔。

将 IP 地址导入全局允许列表：

值栏是用于您想要列入允许列表的 IP 地址 (CIDR 记数法和*, ? 和 *, ?, # 等通配符均支持)，*类型* 栏应该说，"AllowListIPGlobal"，以及*注释* 栏是用于对于每一条目，您可能想加上自己的引用。*"注释"*列是可选的，但若包含了注释列，则不含注释的任意条目都需使用空白引号。

CSV 文件示例：

```
"Value","Type","Comments"
"1.2.3.4"、"AllowListIPGlobal"、"这是关于地址的注释。"
"1.1.1.1","AllowListIPGlobal",""
"192.168.*.*"、"AllowListIPGlobal"、"这是另一个注释。"
```

将 IP 地址导入一个特定域的 IP 允许列表：

*"域"*栏就是用于该允许列表所属之域。例如，如果您想要将地址添加至 example.com 的 IP 允许列表，那么请使用 域栏中的*"example.com"* 。*值 (Value)*列是要加入允许列表的

IP 地址(支持 CIDR 表示法和 *、? 以及 # 通配符)，*类型 (Type)*列应为 "AllowListIPDomain"，而*注释 (Comments)*列是您可能想添加的与该条目有关的任何说明，供自己参考。*"注释"*列是可选的，但若包含了注释列，则不含注释的任意条目都需使用空白引号。

CSV 文件示例：

```
"Domain","Value","Type","Comments"
"example.com"、1.2.3.4"、"AllowListIPDomain"、"这是有关该地址的注释。"
"example.com","1.1.1.1","AllowListIPDomain",""
"example.com"、"192.168.*.*"、"AllowListIPDomain"、"这是另一个注释。"
```

从允许列表导出 IP 地址

要导出一个 IP 允许列表：

1. 在*针对域：*下拉列表框中，选择全局或特定域。
2. 在页面顶部工具栏上点击 *"导出"*。这会打开文件下载对话框。
3. 点击 *"保存"*。
4. 选择文件名称和位置。
5. 点击 *"保存"*，然后是 *"关闭"*。

允许列表条目

该页用于向允许列表中添加新的 IP 地址和编辑现有条目。每当您点击 IP 允许列表中的 *新建* 或者 *编辑*，便会将其打开。

列表项

针对域：
使用该下拉列表框来添加地址到指定域的允许列表，或者若您想要添加地址到全局列表中，请选择全局。

IP 地址：
在此输入 IP 地址，其邮件将不受任何安全功能的约束 (这些安全功能已设置为豁免 "允许列表中所列发件人"或 "允许列表中所列 IP 地址")。支持 CIDR 表示法，也可使用通配符：*、? 和 #，在单个条目中将一组地址列入允许列表。

注释：
在该区域可输入有关该条目的任意注释或说明，供自己参考。

保存与关闭
完成条目编辑后，点击 *"保存并关闭"*将该条目保存到允许列表中。

关闭
如果您希望关闭 "允许列表条目"页面且不作保存，请点击该按钮。

4.10 Sieve 脚本

Sieve 是建议的标准邮件过滤语言，它具备可扩展性，且用途十分广泛。SecurityGateway 在其核心功能中大量使用 Sieve 脚本，把 Sieve 作为邮件内容过滤[195]功能的基础，并支持可用于多种目的的定制脚本。SecurityGateway 使用两类脚本，可在 Sieve 脚本页进行管理：

系统生成的—SecurityGateway 的核心功能是由这些脚本实现的。当通过管理界面更改配置时，在 Sieve 脚本页上会相应修改与被更改的选项相关的脚本。这是修改系统生成脚本的唯一方法；它们具有只读属性，因而不能在 Sieve 脚本页上直接编辑。然而，尽管不能对系统生成脚本自身进行编辑，但可使用与列出的每个脚本关联的向上和向下箭头重新排列它们的处理顺序。

管理员定义的—可使用 Sieve 脚本页自行编写定制脚本，Sieve 提供了非常灵活的过滤方法，因而您可定义任意数量的这类脚本以满足特定需求。然而，要编写这些脚本，需要了解有关 SMTP 和使用 Sieve 过滤语言编写脚本的基本应用知识。SecurityGateway 中的 Sieve 应用包括基本语言、多个标准扩展命令和大量定制扩展命令[230]。

此处以及编写 Sieve 脚本[221]和 SecurityGateway Sieve 控制命令[230]页面上提供了有关 Sieve 及其在 SecurityGateway 中使用方式的基本信息，但对该语言本身的完整介绍则超出了本向导的讨论范围。有关 Sieve 的更多信息，应在线查阅 IETF 网站上的权威文档：Sieve: An Email Filtering Language (RFC-5228)、Sieve's Copy Extension (RFC 3894)、Sieve's Body Extension (RFC-5173)、Sieve's Reject Extension (RFC-5429)、Sieve's Variables Extension (RFC-5229) 和 Spamtest and VirusTest Extensions (RFC-3685)。

Sieve 脚本列表

Sieve 脚本页包含所有系统生成的和管理员定义的脚本列表。该列表包含六个部分：IP、HELO、AUTH、MAIL、RCPT 和 DATA。它们分别对应于 SMTP 处理过程的不同阶段或*邮件事件*，每个脚本各自罗列在其相关部分中。一次处理一个部分的脚本，按其罗列顺序，首先处理全局脚本，然后处理针对特定域的脚本。通过使用与给定脚本相关联的向上和向下箭头更改该脚本在列表中的位置，可以控制每一部分中的脚本处理顺序。

页面顶部的工具栏包含以下三个选项：

新建
点击*"新建"*打开"Sieve 脚本编辑器[220]"，用来编写脚本。

编辑
选择一个脚本，然后在工具栏上点击*"编辑"*，在"Sieve 脚本编辑器[220]"中将其打开。或者，您只需双击脚本即可。系统生成的脚本无法编辑，但仍可在脚本编辑器中将其打开以查看或复制脚本文本并粘贴到新定制规则中。

删除
要删除定制脚本，请在列表中将其选中，然后点击 *"删除"*。随后出现一个对话框，要求您确认删除脚本的决定。系统生成的脚本无法删除。

脚本列表有以下五栏：

启用
该栏针对每个所列脚本有一个复选框，选中或清除相应的复选框可快速启用或禁用脚本。使用该选项只能启用或禁用定制脚本。要启用或禁用系统生成的脚本，必须使用界面上对应于该脚本相关功能的控件（即灰名单、IP 防护、贝叶斯自动学习等）。

作用范围
该栏列出脚本的作用范围。范围可以是 "全局"或特定域。全局脚本作用于所有邮件。针对特定域的脚本只作用于相关域的邮件。

订购
按照脚本的罗列顺序处理脚本。若想更改顺序，可使用该栏内的向上和向下箭头将其重新排列。

脚本名称
这是用来标识脚本的标题或描述性名称。编写定制脚本时将指定该名称。

脚本
将鼠标悬停在该图标上会看到脚本文本显示在工具提示中。若想更透彻地审核脚本文本，可双击该脚本在 Sieve 脚本编辑器 220 中将其打开。

Sieve 脚本编辑器

每当在 Sieve 脚本页工具栏上点击 *"新建"*或 *"编辑"*按钮时，会打开 Sieve 脚本编辑器。它用来编写新的 Sieve 脚本或编辑现有脚本。使用该编辑器草拟或编辑了脚本后，点击工具栏上的 *"保存并关闭"*按钮保存脚本并返回 Sieve 脚本页。

脚本属性

启用对此脚本的处理
该复选框对应于 Sieve 脚本列表中的 *"启用"*栏。默认情况下，脚本编写后即被启用，表示它们被添加到脚本列表中并在下面指定的 *"邮件事件"*中进行处理。若要禁用脚本，请清除该复选框。禁用时，该脚本仍出现在列表中，但不会随其他脚本一起被处理。此外，不能使用该选项启用或禁用系统生成的脚本。它们的管理必须使用各种接口页面上对应于特定脚本的选项来实现。

脚本名称：
使用该文本框指定脚本的标题或描述性名称。系统生成的脚本无法重命名。

邮件事件：
编写脚本时，使用该下拉列表选择邮件事件或 SMTP 会话阶段作为脚本的处理时机。例如，若编写脚本与邮件收件人进行比较，那么应在该选项中选择 RCPT 或 DATA，因为直到 SMTP 会话的 RCPT 阶段才会获悉邮件收件人。六个邮件事件，按其发生顺序列表如下：IP、HELO、AUTH、MAIL、RCPT 和 DATA。

作用范围：
使用该选项指定脚本的作用范围：全局或域。当选择 *"全局"*时，无论邮件发往哪个域，都对脚本进行处理。当选择 *"域"*时，只针对发往指定域的邮件测试脚本。*域*只能在选择上述 RCPT 或 DATA *"邮件事件"*时才可使用，因为在 SMTP 处理过程该阶段之前不知道收件人所在域。

域：
当选择 *"域"*作为脚本的 *"作用范围"*时，会出现该下拉列表。从中选择与该脚本相关联的特定域。

脚本文本：
在此区域，使用 Sieve 邮件过滤语言，输入脚本的实际文本。要获取脚本范例和有关 Sieve 语言的基本信息，请参见：编写 Sieve 脚本 221。

4.10.1 编写 Sieve 脚本

本页，连同 Sieve 脚本 219和 SecurityGateway Sieve 扩展命令 230页，提供了有关 Sieve 邮件过滤语言及其在 SecurityGateway 中应用的基本纲要。本页的第一部分概述了 Sieve 脚本的基本组成部分。下一部分概述了该语言的多种结构单元 222。然后是所支持的标准控制 224、测试 224和操作 227命令的列表。最后，在页面下方提供了多个脚本范例 228供审阅。

要了解有关 Sieve 邮件过滤语言的更详尽说明，应在线查看 IETF 网站的权威文档：Sieve: An Email Filtering Language (RFC-5228)、Sieve's Copy Extension (RFC 3894)、Sieve's Body Extension (RFC-5173)、Sieve's Reject Extension (RFC-5429)、Sieve's Variables Extension (RFC-5229) 和 Spamtest and VirusTest Extensions (RFC-3685)。

还可访问 www.mdaemon.com/Support/ 了解 SecurityGateway 的最新技术支持和帮助选项，包括：电话支持、邮件支持、知识库、常见问题解答和社区论坛等。

Sieve 脚本的组成部分

Sieve 脚本有四个基本组成部分：

1. **需求**—该部分用于声明给定脚本所需的 Sieve 扩展命令。如果脚本中要使用可选的扩展命令，则必须使用 require 控制命令在脚本开头列出所需的那些扩展命令。require 命令的参数末尾需添加分号。

   示例：

   ```
   require "securitygateway";

   -and-

   require ["securitygateway", "fileinto"];
   ```

2. **条件**—在脚本的这一部分中可说明在邮件中要查找的内容特定类型以及测试并比较这些内容的方式。

   示例：

   ```
   if size :over 1M
   ```

   -and-

   ```
   if header :contains ["to", "cc"] "Frank Thomas"
   ```

3. **操作**—该部分为当指定条件为“true”时要实施的操作和要执行的命令。每一操作必须后接分号，且每一组操作必须包含在大括号内（即 "{" 和 "}"）。

   示例：

   ```
   if size :over 1M { discard; }
   ```

   -and-

   ```
   if header :contains ["to", "cc"] "Frank Thomas" {
   bayes-learn "spam";
   fileinto "spam";
   }
   ```

4. **注释**—可以在 Sieve 脚本中包含注释供自己参考，以提醒自己该脚本的功能等等。有两种注释可供使用：单行注释和多行注释。单行注释以 "#" 开头并一直延续到行末（即至下一个 CRLF）。多行注释以 "/*" 开头，可跨越多行文本，然后以 "*/" 结尾。

   示例：

   ```
   # 删除超过 1 mb 的邮件
   if size :over 1M { discard; }
   ```

   -and-

   ```
   if header :contains "from" "Frank Thomas" {
   /* Frank Thomas 常常给我们发送垃圾邮件，因此该脚本
   自动将自他那儿收到的所有内容移入
   用户隔离队列。*/
   fileinto "spam";
   }
   ```

结构单元

字符串
文本字符串开头和结尾使用单个双引号。例如："Frank Thomas".

要在用引号括起来的字符串中包含反斜杠或双引号，必须在该字符前添加另一个反斜杠。因此，在用引号括起来的字符串中，\\ 将被视为 \ 且 \" 将被视为 "。字符串中的其他字符无需换码。

字符串列表
每当您希望在脚本中使用一组字符串时，请用逗号分隔各条用引号括起来的字符串，并将该组字符串用方括号括起来。

示例：

```
if header :contains ["to", "cc"] ["me@xyz.com", "you@xyz.com",
"us@xyz.com"]
```

如果 To 或 CC 报头包含以上三条地址中的任一条，该测试结果即为 True。

报头
报头名中不得包含冒号。

示例：

```
if header :is "to:" (无效)
if header :is "to" (有效)
```

测试列表
类似于字符串列表，脚本中可包含一组测试（用小括号括起来）。当使用 allof 或 anyof 测试命令时，有时必须包含小括号，因为它们分别是逻辑“与”和逻辑“或”语句。

示例：

```
if anyof (size :over 1M, header :contains "subject" ["big file",
"mega file"])
{
discard;
}
```

参数和匹配类型
大多数命令带有一个或多个参数，以便您指定如何操作。参数类型有多种，如位置参数、标记参数和可选参数。举例来说，标记参数和匹配类型参数前加有冒号。:contains、:is、:matches、:over 和 :under 都属于标记参数。某些标记参数仅限于特定命令。有关不同类型参数的更多信息，请参见：RFC-5228。

操作
每一操作必须后接分号，且每一组操作必须包含在大括号内。

示例：

```
if header :contains ["to", "cc"] "Frank Thomas" {
bayes-learn "spam";
fileinto "spam";
}
```

控制命令

Sieve 语言中使用三种控制命令：

require
在脚本开头使用该控制命令来声明在脚本中所用的可选扩展命令。

示例：

```
require ["securitygateway", "fileinto"];
```

if / elsif / else
if 命令是核心控制命令。尽管理论上有三条相互关联的命令，但 elsif 和 else 的使用不能独立于 if。当在脚本中遇到 if 命令时，将评估该测试条件以判断它是否为 true。如果为真，则将执行与之相关的操作。

如果 if 测试结果为 false，则评估第一条 elsif 测试。如果 elsif 为 true，则执行与该测试相关的操作。如果 elsif 测试仍为假，则继续对下一条 elsif 进行评估，依次类推，直到其中一条为真。

如果 if 和所有 elsif 测试都为 false，并有一条 else 命令，则将执行该命令的操作。

stop
stop 控制命令终止所有处理。

测试命令

这些是在 SecurityGateway 的 Sieve 应用中支持的标准测试命令。然而，body 和 envelope 命令是扩展命令，因此每当您希望在脚本中加以使用时，就必须将其包括在 require 控制命令中。此外，在 securitygateway 扩展命令中还包括了大量其他的测试命令，在 SecurityGateway Sieve 扩展命令 230页上对之作了概述。

address
使用该命令，可以只对报头中的邮件地址而不是可能包含的短语或名称进行测试。例如，如果 "to" 报头包含 "Frank Thomas" <frank@example.com>，那么 header :is "to" "frank@example.com" 的测试结果为 false。但是 address :is "to" "frank@example.com" 的测试结果为真，因为在该评估中只考虑地址。

使用该命令时还有三个可选标记参数：":localpart"，":domain" 和 ":all"。:localpart 参数只评估地址的左半部分（例如 "frank@example.com" 中的 "frank"），:domain 参数只使用地址的域部分（例如 "example.com"），而 :all 使用整个地址。若未包含以上参数，则默认使用 :all。

示例：

```
require "fileinto";
if address :domain :is "from" "spammer.com" {
fileinto "spam";
}
```

allof
该测试为逻辑“与”，表示所有的评估条件都必须为真才能执行操作。

示例：

```
if allof (header :contains "from" "J.Lovell", header :contains "to"
"Bubba")
{
fileinto "spam";
}
```

anyof
该测试为逻辑“或”，表示若评估条件部分为真就能执行相关操作。

示例：

```
if anyof (size :over 1M, header :contains "subject" "big file
attached")
{
reject "I don't want messages that claim to have big files.";
}
```

body
body 测试命令是可选的扩展命令，因而在要使用它的脚本开头必须添加 require "body" 这个控制命令。该命令比较邮件正文。有关该命令的更多信息，请参阅：Sieve's Body Extension (RFC-5173)。

示例：

```
require ["body", "fileinto"];
if body :text :contains "secret formula" {
fileinto "admin";
}
```

envelope
envelope 命令是可选的扩展命令，因而在要使用它的脚本开头必须添加 require "envelope" 控制命令。当 "from" 或 "to" 分别用作命令参数时，该命令比较信封部分的 SMTP 发件人和收件人。

示例：

```
require "envelope";
if envelope :is "from" "MrsFrank@company.com" {
redirect "frankshome@example.com";
}
```

exists
若邮件中存在参数中所列报头，该测试为真。列出的所有报头必须全都存在，否则该测试为假。

示例：

```
if exists "x-custom-header" {
redirect "admin@example.com";
}
-and-
if not exists ["from", "date"] {
discard;
}
```

false
该测试评估结果始终为“FALSE”。

header
当指定报头的数值匹配参数所设置的条件时，该报头测试评估结果为 true。当未指定匹配类型参数时，默认使用 :is。

示例：

```
require "fileinto"
if header :is "x-custom-header" "01" {
fileinto "admin";
}
```

not
将该命令随其他测试一起使用意味着测试结果必须求反才能执行该测试的相应操作。例如，测试 if not exists ["from", "date"] { discard; } 表示如果邮件既不包含 "from" 也不包含 "date" 报头，则执行 discard 操作。如果省略 not 命令，则表示当这些报头果真存在时删除该邮件。

size
size 命令接受标记参数 ":over" 和 ":under"，且其后必须跟一个数值。该参数用于指定邮件大小必须大于还是小于指定数值才能使测试结果为真。可在数值后使用 M 表示兆字节，K 表示千字节，或不带任何字母表示字节。

示例：

```
if size :over 500K {
discard;
}
```

true
该测试评估结果始终为“TRUE”。

spamtest
spamtest 命令是可选的 Sieve 扩展命令，相关论述包含在 Spamtest and VirusTest Extensions (RFC-3685) 这篇文档中，位于 ietf.org。请查看该文档了解有关该扩展命令的信息。

virustest
virustest 命令是可选的 Sieve 扩展命令，相关论述包含在 Spamtest and VirusTest Extensions (RFC-3685) 这篇文档中，位于 ietf.org。请查看该文档了解有关该扩展命令的信息。

操作命令

这些是 SecurityGateway 支持的标准操作命令。fileinto 和 reject 命令是扩展命令，因此每当您希望在脚本中加以使用时，就必须将其包括在 require 控制命令中。securitygateway 扩展命令中还提供了许多其他操作命令，在 SecurityGateway Sieve 扩展命令 230 这个页面上对其作了概述。

fileinto
fileinto 操作命令是可选的扩展命令，因而在要使用它的脚本开头必须添加 require "fileinto" 这个控制命令。该命令接受两个参数："spam" 和 "admin"。"spam" 将邮件移入用户隔离 255，而 "admin" 将它移入管理员隔离 256。

示例：

```
require "fileinto";
if header :contains "from" "Frank Thomas" {
fileinto "spam";
}
```

discard
该操作导致邮件被自动删除，而不会发送投递状态通知和任何其他消息。

示例：

```
if size :over 2M { discard; }
```

keep
该操作导致邮件被保存到默认位置。

redirect
该命令把邮件改投到相关参数中指定的地址，而不会更改邮件正文和现有报头。该命令还支持可选的 :copy 扩展参数，它将邮件的副本发送到指定地址而不是重新投递该邮件。因而在将副本发送到指定地址以外，还可执行其他操作。

示例：

```
require "copy";
if header :contains "subject" "Response to XYZ" {
redirect :copy "offers@example.com";
bayes-learn "ham";
}
```

reject
reject 操作命令是可选的扩展命令，因而在要使用它的脚本开头必须添加 require "reject" 控制命令。该命令导致在 SMTP 处理过程中邮件被拒绝，并附带 5xx 响应代码和参数中指定的可选短消息。

```
require "reject";
if size :over 5M {
reject "No way! This message is too big for me to accept.";
}
```

vnd.mdaemon.securewebmsg
使用这个操作命令来使用 SecurityGateway 的安全通信 web 门户来发送邮件。

示例：

```
require
["securitygateway","reject","fileinto","envelope","body","regex"];
if allof(header :matches "subject" "[Secure Message]*")
{
vnd.mdaemon.securewebmsg;
}
```

Sieve 脚本范例

拒绝主题中包含 "[SPAM]" 的任何邮件

```
require "reject";
if header :contains "subject" "[SPAM]"
{
reject "I don't want your spam";
}
```

拒绝发往特定实名的任何邮件

```
require ["securitygateway","reject"];
if header :contains "to" "Real Name"
{
bayes-learn "spam";
reject "I don't want your spam";
}
```

定制贝叶斯自动学习

```
require ["securitygateway","comparator-i;ascii-numeric"];
```

如果被列入允许列表

```
{
bayes-learn "ham";
}
elsif anyof(blocklisted,spamtotal :value "gt" :comparator "i;ascii-numeric" "20.0")
{
bayes-learn "spam";
}
```

GreylistDNSBL 匹配

```
require ["securitygateway"];
if not lookup "rblip" "all" {greylist;}
```

收到大型邮件时通知管理员

```
require ["securitygateway"];
if size :over 1M
{
alert text:
收件人：admin@company.mail
发件人：postmaster@$RECIPIENTDOMAIN$
主题：SecurityGateway 内容过滤器邮件
X-Attach-Msg: No
$RECIPIENT$ 收到超过 1MB 的邮件。
.
;
}
```

当主题以“Secure Message]”开头时作为安全邮件发送

```
require ["securitygateway","reject","fileinto","envelope","body","regex"];
if allof(header :matches "subject" "[Secure Message]*")
{
vnd.mdaemon.securewebmsg;
}
```

4.10.2 Sieve 扩展命令

要使用 SecurityGateway 的定制 Sieve 扩展命令，就必须在会用到该命令的脚本开头包括以下 require 命令：

```
require "securitygateway";
```

测试命令

ip

ip 测试的执行时机可以是 SMTP 处理过程中的任何阶段（即任何邮件事件 220 中）。

- **cidr**—第二个参数是要与客户端 IP 地址进行比较的 IP 地址或模式。可以是确切的 IP 地址，用 CIDR 指定的范围（如 10.0.0.0/24），或通配符模式：其中 ? （任何单个字符），* （0 个以上字符），# （1 位以上数字）（例如 10.*.*.*）。

  代码示例：`if not ip :cidr "10.0.0.0/24" { greylist; }`

- **public**—如果客户端 IP 地址不属于 RFC-1918 私有子网，也不是回环地址或 DHCP 自动 IP 地址，则为 true，否则为 false（127.0.0.0/8、192.168.0.0/16、10.0.0.0/8、172.16.0.0/12、169.254.0.0/16）。

  代码示例：`if ip "public" { greylist; }`

- **private**—public 的逻辑求反。
- **ssl**—若客户端已成功建立了安全的（SSL）连接，则为 true
- **des**—若客户端为域邮件服务器，则为 true

lookup

何时可调用 lookup 测试取决于第一个参数：

- **ptr**—当它为第一个参数时，可随时执行 lookup 测试。第二个参数可以是标准的标记参数或 "resolves"、"resolvestoclient" 或 "error"。

  例如：`if lookup "ptr" :matches "*.domain.com" { greylist; }.`

  - **resolves**—若存在 PTR 记录，则返回 true。
  - **resolvestoclient**—返回 true，若 PTR 记录匹配的话 - 即 PTR 主机的 A 记录查找返回了客户端的 IP 地址。
  - **error**—若发生临时 DNS 查询错误，则返回 true。

- **helo**—当它为第一个参数时，只能在 HELO 事件中或之后执行 lookup 测试。第二个参数可以是 "resolves"、"resolvestoclient" 或 "error"。
  - **resolves**—若 HELO 参数为有效 IP 地址或主机名，则返回 true。
  - **resolvestoclient** - 返回 true，若 HELO 参数匹配的话 - 即 HELO 参数的 A 记录查找返回了客户端的 IP 地址。
  - **error** - 若发生临时 DNS 查询错误，则返回 true。

- **mail**—当它为第一个参数时，可在 MAIL 事件中或之后执行 lookup 测试。第二个参数可以是 "resolves"、"resolvestoclient"或 "error"。
  - **resolves**—若 MAIL FROM 域为有效域，则返回 true。
  - **resolvestoclient**——返回 true，若 MAIL FROM 域匹配的话 -即 MAIL FROM 域的 A 记录查找返回客户端的 IP 地址。
  - **error**—若发生临时 DNS 查询错误，则返回 true。
- **spf**—当它为第一个参数时，可在 MAIL 事件中或之后执行 lookup 测试。第二个参数可以是 "pass"、"fail"或 "error"。
  - **pass**—若发件人通过了 SPF 验证则返回 true，若验证结果不确定或失败则返回 false。
  - **fail**—若发件人未通过 SPF 验证则返回 true，若验证结果不确定或通过验证则返回 false。
  - **error**—若处理过程中出错 (通常为 DNS 查询错误)则返回 true
- **rblip**—当它为第一个参数时，可随时执行 lookup 测试。第二个参数可以是 "all"、"any"或 "error"。
  - **all**—如果客户端 IP 地址通过了所有 DNS 阻止列表检测，则返回 true
  - **any**—如果客户端 IP 地址通过了任何 DNS 阻止列表，则返回 true。
  - **error**—若处理过程中出错 (通常为 DNS 查询错误)则返回 true
- **rblhdr**—当它为第一个参数时，只能在 DATA 事件中执行 lookup 测试。第二个参数可以是 "all"、"any"或 "error"。
  - **all**—如果已接收报头通过了所有 DNS 阻止列表检测，则返回 true
  - **any**—如果已接收报头地址通过了任何 DNS 阻止列表，则返回 true。
  - **error**—若处理过程中出错 (通常为 DNS 查询错误)则返回 true

port

port 测试可随时执行。唯一的参数是端口号，用来与客户端连接的实际端口进行比较。

代码示例：`if port 25 { greylist; }`

auth

何时可调用 auth 测试取决于第一个参数：

- **succeeded**—若身份验证成功则为 true。当它为第一个参数时，可在 AUTH 事件中或之后执行 auth 测试。
- **match**—若身份验证成功且 MAIL FROM 地址与经过身份验证的账户相匹配，则为 true。当它为第一个参数时，可在 MAIL 事件中或之后执行 auth 测试。

verify

verify 测试验证地址（参见：用户验证源 52）。不同于所有其他测试，即使在 sieve 过滤器中未包含相应代码，该测试也始终会执行。也就是说，对每条 MAIL FROM 和 RCPT TO 地址进行验证并缓存结果。何时可调用 verify 测试取决于第一个参数：

- **from**—若 MAIL FROM 地址为有效本地地址，则为 true。当它为第一个参数时，可在 MAIL 事件中或之后执行 verify 测试。
- **fromdomain**—若 MAIL FROM 地址来自有效本地域，则返回 true。当它为第一个参数时，可在 MAIL 事件中或之后执行 verify 测试。
- **fail_from**—若验证 MAIL FROM 地址时出错则为 true。当它为第一个参数时，可在 MAIL 事件中或之后执行 verify 测试。
- **to**—若 RCPT TO 地址为有效本地地址，则为 true。当它为第一个参数时，可在 RCPT 事件中或之后执行 verify 测试。
- **todomain**—若 RCPT TO 地址指向有效本地域，则为 true。当它为第一个参数时，可在 RCPT 事件中或之后执行 verify 测试。
- **fail_to**—若验证 RCPT TO 地址时出错则为 true。当它为第一个参数时，可在 RCPT 事件中或之后执行 verify 测试。

dkim

dkim 测试检查 DomainKeys Identified Mail (DKIM) 154 验证，并只能在 DATA 事件中执行。

- **pass**—若邮件由 DKIM 签名且该签名通过了验证，则返回 true。
- **fail**—若 DKIM 处理返回硬失败，则为 true。（需要使用 SSP 选项）
- **error**—若 DKIM 处理出错则返回 true。

cbv

cbv 测试可在 MAIL 事件中或之后执行。在不含参数的情况下，它返回 true，只要 MAIL FROM 地址通过 回叫验证 169。

- **error**—若 CBV 处理出错则返回 true。

spamtotal

spamtotal 测试检查邮件分数 143 并可在任何事件中执行。然而，在大多数情况下，应在 DATA 事件的最后一个过滤器中运行该测试，以便所有其他过滤器都能为邮件打分，以合成最后的邮件分数。

spamtotal 测试具有单个参数：阈值。若邮件分数不小于阈值，该测试返回 true，否则返回 false。

OutbreakProtection

OutbreakProtection 测试只能在 DATA 事件中执行。在不含参数的情况下，若爆发保护 126 将邮件归类为垃圾邮件、病毒或群发邮件，该测试返回 true。

- **spam**—若爆发保护将邮件归类为垃圾邮件，则返回 true。
- **virus**—若爆发保护将邮件归类为包含病毒，则返回 true。
- **phish**—若爆发保护将邮件归类为网络钓鱼邮件，则返回 true。
- **suspect**—若爆发保护将邮件归类为疑似垃圾邮件，则返回 true。
- **bulk**—若爆发保护将邮件归类为群发邮件，则返回 true。
- **error**—若爆发保护处理出错则返回 true。

allowlisted

该测试有一别名：exempt（为了向后兼容）。何时执行该测试取决于第一个参数：

- **all**——与不含参数作用相同；如果客户端被列入允许列表[212]，则返回 true。可在任何事件中调用，且只使用现有的信息。例如，当在 IP 事件（第一个事件）中调用时，只比较允许列表中匹配 PTR 记录的 IP 地址和主机。
- **ip**—如果客户端被列入 IP 地址允许列表[217]，则返回 true。可在任何事件中执行。
- **host**—如果客户端被列入主机允许列表[215]，则返回 true。可以是匹配 HELO 参数或 PTR 主机。可在 HELO 事件中或之后执行。
- **mail**—如果 MAIL FROM 被列入地址允许列表[213]，则返回 true。可在 HELO 事件中或之后执行。
- **from**—返回 true，若 From：报头被列入地址允许列表[213]。只能在 DATA 事件中执行。

blocklisted

该测试有一个别名：黑名单（用于向后兼容）。参数和功能类似于 whitelist 测试，只是比较对象为阻止列表[205]。

操作命令

error

error 命令类似于 RFC 3028 中定义的 reject 命令，只是它有 2 个参数。第一个参数为 SMTP 错误代码，第二个参数为文本消息。两者都要发送以响应当前客户端命令。

disconnect

disconnect 命令类似与 “error”命令，只是它还关闭了 TCP/IP 套接字。这与 MD 中的关闭选项很相似。

greylist

greylist 命令激活灰名单登记[140]。

dynamicscreen

dynamicscreen 命令激活动态屏蔽[177]。

tarpit

tarpit 命令激活缓送[179]。

sign

sign 命令为邮件添加签名[155]报头。第一个参数可以是：

- **dkim**—由 DKIM[155] 为邮件签名。第二个参数是要使用的选择器名称。

throttle

throttle 命令激活带宽节流[180]。第一个参数是以“字符/秒”为单位的带宽限制。

ipshield

ipshield 命令激活 IP 屏蔽[176]。

spamscore

spamscore 命令将第一个参数添加到邮件的当前邮件分数[143]总额上。参见 spamtotal 测试。

tagheader

tagheader 命令在邮件中的某个报头前添加标记。第一个参数是要修改的报头。第二个参数是要在报头值中插入的文本。

addheader

addheader 命令为邮件添加新报头。第一个参数是要添加的报头，第二个参数是报头值。

removeheader

removeheader 命令从邮件中删除报头。第一个参数是要删除的报头。

alert

alert 命令发送通知。唯一的参数是包含 from:、to:、subject: 和其他报头的邮件主体。整个字符串取决于宏扩展。

changesender

changesender 操作用于更改 SMTP MAIL FROM 命令的值，SecurityGateway 在投递邮件时会使用该命令。例如，在使用仅内部域名时，可以使用此名称；当在域外发送邮件时，必须更改此名称。

示例：

```
require ["securitygateway", "envelope"];
if envelope :matches "From" "frank@internal.mail"
{
changesender "frank@example.com";
}
```

execute

- 该脚本必须放在“Sieve Executable Path”目录中，可以从“设置 » 系统 » 目录[109]”进行配置。可以将“execute”这个 sieve 关键字用作操作和测试。
- 第一个参数是脚本的名称。支持 .bat、.exe 和 PowerShell。
- 第二个参数是将传递给进程的参数。message_filename sieve 变量填充了当前正在处理的邮件的 RFC822 源的完整路径。
- Sieve 变量 ${vnd.mdaemon.execute.exit_code} exposes the exit code of a process executed 通过 execute 命令来公开执行的进程的退出代码。只有在完成 execute 命令后该变量才可用。

示例：

```
require ["securitygateway","relational","comparator-i;ascii-
numeric"];
execute "Test.ps1" "-msg '${message_filename}'";
```

将记录处理的每封邮件的文件名的 PowerShell 脚本的文本是...

```
param
(
    [string]$msg = ""
)

Add-Content -Path "c:\files_processed.txt" -Value $msg
Write-Host $msg
```

示例 2:

```
require ["variables", "securitygateway"];


execute "some-script.bat";


if string "${vnd.mdaemon.execute.exit_code}" "1" {
 fileinto "spam";
} elsif string "${vnd.mdaemon.execute.exit_code}" "2" {
    reject "This message looks like spam";
}
```

章节

5

5 AI 分类

AI 分类是一项值得注意的功能，使您能够利用人工智能分析邮件内容，并对邮件进行分类。这涉及将邮件数据（如标题和正文内容）发送给第三方 AI 供应商（或使用本地 AI 模型处理）以进行分析。然后，基于该分析，可以为邮件分配分类或类别，例如合法、网络钓鱼、商业、垃圾邮件、PII_DETECTED 等。您可以设置规则来确定将分析哪些邮件，以及将根据生成的 AI 分类采取哪些操作。如果您组织的策略允许以这种方式处理数据，则此功能可以提供明显的优点，例如：

- **高级威胁检测** — 识别传统过滤器可能错过的复杂网络钓鱼尝试。
- **敏感内容识别** — 检测包含个人身份信息（PII）或其他敏感数据的邮件。
- **改进的过滤** — 更准确地过滤不需要的邮件（例如未经请求的商业电子邮件）。

配置 AI 分类

可以从以下页面配置 AI 分类：

模型 238 — 使用此页面可管理用于分析所选邮件的 AI 模型列表。您可以添加、编辑或删除模型，并查看其配置详细信息，如名称、终端 URL、AI 配置文件、超时和 API 密钥。

提示词 240 — 创建和管理当邮件与给定的规则匹配时，将发送到所选 AI 模型的提示词。

规则 243 — 您可以在此页面创建规则来确定要分析哪些邮件、要发送哪些提示词，以及要根据分配给邮件的结果分类标签采取哪些操作。

5.1 模型

使用此页面可管理用于分析所选邮件的 AI 模型列表。您可以添加、编辑或删除模型，并查看其配置详细信息，如名称、终端 URL、AI 配置文件、超时和 API 密钥。您可以选择使用基于云的 AI 模型和您自己的本地托管模型。

基于云的 AI 模型

以下是选择基于云的 AI 模型时需要考虑的一些事项。

成本和测试考量

在使用基于云的 AI 模型时，成本是一个需要考虑的问题，因此您应该测试各种模型，看看哪种模型最适合您。您可能会发现使用下方推荐的模型的成本相当易于管理，特别是在将AI 规则 243配置成限制哪些所发邮件用于分类。例如，您可以选择仅对发送给某些用户的邮件使用 AI 分类，例如您认为可能最容易受到网络钓鱼威胁的邮件。

OpenAI API — OpenAI 可以为新账户提供一定数量的免费令牌。对于更广泛的测试，或者如果您同意他们的数据使用策略（可能涉及允许他们将您的数据用于培训目的），您可能会找到降低成本或免费测试的选项。始终查看任何 AI 供应商的当前服务条款。

Google Cloud AI——通过免费的 Google Cloud 账户，Google 通常会提供有限数量的免费请求作为其免费套餐的一部分，这对于初始测试和熟手非常有用。

推荐基于云的 AI 模型

为了实现能力和性价比的最佳平衡，请考虑以下模型：

1. **OpenAI**:
   - **gpt-4.1-mini** — 对于常规任务而言 很好地平衡了性能和性价比。
   - **gpt-4.1** — 更强大的选项，可能更适合复杂的分析，但可能会产生更高的成本。
2. **Google Gemini**:
   - **gemini-2.0-flash** — 其设计旨在速度和高效。

本地 AI 模型

如果向第三方发送数据不可行，则支持 OpenalAPI 的本地 AI 模型也是一种选择。能过促成这一点的一些平台包括：

LocalAI

Ollama (OpenAI Compatibility)

对于本地模型，性能将是一个值得考虑的问题，特别是如果您没有专用的 GPU 或 AI 加速器硬件的情况下。在细致入微的任务 例如准确检测邮件是网络钓鱼还是纯粹商业）方面，本地模型的能力通常不如领先的云模型。但是，它们对于其他用例可能非常有效，例如根据您定义的特定内容模式标记邮件。

添加或编辑 AI 模型

要将新的 AI 模型添加到模型 238 列表，请点击模型页面工具栏上的**新建**。要编辑现有的模型条目，请选择该条目并点击 **编辑**”。

属性

配置文件：
选择内置的 AI 配置文件，或选择**自定义**，以便在使用不同的 AI 模型时输入您自己的设置。

显示名称：
为这个 AI 模型的条目输入一个名称；这个名称只是供您参考。对于预定义的配置文件，将为您添加一个通用名称，如果您愿意，可以更改该名称。

终端 URL：
这是可以访问 AI 模型的 API，以发送请求和接收响应的特定 web 地址。在大多数情况下，当您选择上方的*配置文件*，就会为您自动添加这个 URL。

API密钥：
使用此选项提供从您选择的 AI 服务供应商获得的任何必要的 API 密钥。

模型名称：
输入一个模型名称或点击**刷新列表**来生成可用模型的下拉列表。

刷新列表
点击此按钮可生成可用 AI 模型的下拉列表。**请注意：**您必须先输入*终端 URL* 和 *API 密钥*来使用*刷新列表*选项。

超时（秒）：
这是服务器在放弃之前等待 AI 响应的秒数。

默认语气：
AI 分类的默认语气被设置为 1.0。语气参数控制 AI 响应的随机性，范围为 0 到 2。例如，0.1 的语气将非常狭隘局限，且具有确定性，这可能会由于极端的刚性而导致错误的分类。相反，2.0 的设置将是高度随机的，可能会产生奇怪的，不相关的，甚至是荒谬的结果。在大多数情况下，您应该将此设置保留为默认值 1.0。如果您经常遇到不正确的分类，您应该首先尝试调整提示词 240，而不是语气设置。

允许无效的 SSL 证书
在使用本地或自定义*配置文件*时，如果您希望允许无效的 SSL 证书，请选中此框。

额外的 HTTP 请求报头：
如果您需要包含任何其他 HTTP 请求报头，请在此处输入这些报头。

测试连接

一旦配置了您的 AI 模型，请点击对话框顶部的**测试连接**来确保您的服务器连接到配置的 AI 模型并获得响应。

5.2 提示词

使用此页面来创建和管理 AI 分类 238 提示词，这些提示词将被发送到您选定的 AI 模型 238，时机是当邮件匹配您的 AI 分类规则 243。您可以添加、编辑和删除提示词，并查看每个提示词的配置详细信息。该“提示词列表”显示*已启用*列，用于启用/禁用提示词，此外还包括*提示词名称*列，以及显示提示词正在使用哪个 AI *模型*的列。

添加或编辑 AI 提示词

要将新的 AI 提示词添加到提示词 240 列表，请点击提示词页面工具栏上的**新建**。要编辑现有的提示词，请选择这个提示词条目，并点击“**编辑**”。

属性

启用
选中此框可为用户启用所选提示词。

名称：
为提示词指定唯一名称。

描述：
使用此框来描述提示词。这是可选的，仅供您参考。

AI模型：
使用这个下拉列表来选择将收到提示词的预配置 AI 模型 238。

提示词文本：

这是将发送至选定 *AI 模型*的文本，时机是当邮件匹配了与该提示词关联的 AI 分类规则[243]。该提示词必须询问模型来为每封分析过的邮件返回其中一个在下方指定的*已允许分类标签*，可以选择在逗号后跟随一些额外的文本。提示词中提到的标签必须与您在该选项中指定的标签完全匹配，否则邮件可能无法正确分类。提示词中有许多变量可供使用，以准确控制该提示词中包含哪些邮件数据。点击**查看所有可用变量**来查看这些变量列表。还请参阅下方的示例提示词[242]来获取可接受提示词的两个示例，每个示例都有解释说明。

查看所有可用变量
点击此按钮可显示提示词中允许的所有变量的列表。变量必须用大括号括起来：例如：{variable_name}。要设置变量允许的最大字符数，请使用：{variable_name,max_chars}. 例如：{body.text,50000} 将替换变量的文本的大小限制为 50,000 个字符。超出该范围的任何文本都将被截断。

变量	描述
{classification_labels}	允许的分类标签
{remote_ip}	远程客户端 IP 地址
{remote_ip.ptr}	PTR（反向 DNS）记录
{ehlo_domain}	EHLO/HELO 域
{ehlo_domain.ptr}	EHLO/HELO 域（反向 DNS）
{env_from}	信封发件人地址
{subject}	电子邮件主题
{body.text}	纯文本邮件正文
{body.html}	HTML 邮件正文
{attachments}	附件列表
{headers}	邮件报头(已解码)
{headers.raw}	邮件报头（raw）
{message.raw}	完整原始邮件数据（RFC 5322）

查看示例提示词
点击此按钮可查看示例提示词，可用作创建 AI 分类提示词的模板或起点。在该页面，请点击*"使用此模板"*按钮来将示例提示词复制到下方的*"提示词文本"*框中。还请参阅：示例提示词[242]来了解有关如何构建提示词的更多信息。

已允许分类标签：

这些是您将提示词 AI 分配给分析的邮件的分类标签。如果您在提示词中手动定义分类标签，而不是使用 *{classification_labels}* 变量，则它们必须准确匹配这些标签。如果提示词中的标签与此处指定的标签不匹配，则邮件将无法正确分类。

示例提示词

下方是两个示例 AI 分类提示词。第一个实例比较简单，第二个示例更复杂。**提示：**像 ChatGPT 这样的 AI 工具有助于建议和改进各种分类任务的提示词。

提示词示例 #1:
借助此提示词，AI 模型完全自行确定所列分类的定义。例如，如果您的分类是 LEGITIMATE、SPAM 和 SUSPICIOUS，那么它留给模型来确定什么构成 "垃圾邮件"，什么使邮件 "合法"，以及它认为是 "可疑"的详细信息。该示例还使用 *{classification_labels}* 变量来自动包含您的 *"已允许分类标签"*。请注意，它还指示该模型以 "其中一个正确的"标签响应，"后跟逗号和解释说明。"对于 AI 分类，该模型必须仅返回其中一个分类标签，并可选地在逗号后返回一些附加文本，例如解释为什么将该分类分配给这封邮件。最后，这些变量用于包含要分析的数据：邮件的报头，至多 50,000 个字符的邮件 html 正文，以及包含任何附件的列表。

--

分析该电子邮件，并根据内容分类。以下方正确的标签响应：
{classification_labels}，后跟逗号和解释说明。

报头：{headers}

正文：{body.html,50000}

附件：{attachments}

提示词示例 #2:
在此提示词中，每个分类都是在提示词中定义的；它不留给模型来确定每个分类的含义。它还告诉该模型只用一个分类或类别来响应，然后是逗号和解释说明。告诉该模型为什么选择该分类，有时可以产生更好的结果，减少错误感知或不合逻辑的答案。此外，还会记录额外信息，这可能有助于您解决问题或优化提示词。最后，这些变量用于包含邮件的报头，以及多达 50,000 字符数的邮件正文。

--

您是电子邮件分类助理。您的任务是阅读电子邮件，并将其分类为以下类别之一：

LEGITIMATE（合法）：来自可信来源的个人、工作相关、事务性或预期的电子邮件（例如收据、订单确认和服务更新等）。

UNSOLICITED（未经请求）：不是明确有害或出售某些东西的未请求的电子邮件，例如时事通讯、问卷调查或随机联系尝试。

COMMERCIAL（商业）：推广或销售产品或服务的电子邮件，包括广告、优惠和市场营销活动。

HARMFUL（有害）：看似网络钓鱼尝试、包含恶意软件、冒充已知品牌或服务窃取信息、涉及诈骗或具有恶意意图的电子邮件。只有在有明确的欺骗、欺诈或威胁证据的情况下才使用此标签。来自符合 DMARC 的知名公司的电子邮件不应被标记为有害，除非它们显示出模拟或恶意内容的迹象（例如，不匹配的链接、可疑附件、敦促通过未知 URL 立即登录）。

只用一个类别后跟逗号和解释说明来响应。

报头：{headers}

正文：{body.text,50000}

5.3 规则

您可以在此页面创建 AI 分类238规则来确定要分析哪些邮件、要发送哪些提示词，以及要根据分配给邮件的结果分类标签采取哪些操作。规则列表有以下三列：*已启用*、*规则名称*和*提示词*。*已启用*列包含了一个用于每个条目的选择框，可以用来快速地启用/禁用规则。在创建规则时指定*规则名称*，然后*提示词*列将显示您与规则关联的提示词240的名称。该页面的工具栏具有用于创建、编辑或删除规则的选项。

添加或编辑 AI 规则

要创建一条新规则，点击 "规则"工具栏上的 **"新建"**，然后逐一（顶部到底部）配置编辑器选项。完成后，点击 **"保存并关闭"**来创建新规则。要编辑一个规则，请选择列表中的规则并点击 **"编辑"**。

属性

已启用该规则
要创建一条新规则，必须勾选此框。至于现有的规则，您可以取消勾选此框将此规则禁用。在测试邮件时，SecurityGateway 不会使用已禁用的规则。该选项所响应的是 "规则"列表中的 *"已启用"*列。

针对域：
使用此选项来选择该规则所适用的域。如果选择了 "--全局--"，那么发送至或者来自于您 SecurityGateway 的一切域的全部邮件都将按照该规则进行测试。如果选择的是一个特定域，那么只需测试发送至或来自于该特定域的邮件。

规则名称：
在此输入规则的描述性名称。该选项对应的是 "内容过滤规则"列表上的 *"描述"*栏。

AI提示词：
使用下拉列表来选择在规则引起邮件被分析时，将使用哪个预配置的提示词240。

要执行 AI 提示词的条件：

只有满足以下条件时，才会执行提示词：

所有条件都符合（与）
如果您希望只有当一封邮件满足了所有您所提供的如下测试条件后再匹配一条规则的话，请选择此选项。这是在测试条件下执行一个合乎逻辑的 "与"。换句话来说，"若条件 A 是真的且条件 B 也是真的，那么就执行特定操作。"

...大约 [xx] 字符数以内
启用此项时，仅在*待比较项目*是正文时才应用，其中还包括 SecurityGateway 能够从中提取文本的附件。如果正文存在多个条件，那么所有这些条件都必须在彼此的指定接近度（之前或之后的字符数）内找到。匹配必须全部发生在同一个 mime 部分中，即邮件正文、备选正文或附件。在 "AND" 中包含的其他条件必须为 true，不过无需彼此接近。

符合任意条件（或）
如果您希望一封邮件满足了您所提供的如下测试条件中的任意一项后再匹配一条规则的话，请选择此选项。这是在测试条件下执行一个合乎逻辑的 "或"。换句话来说，"若条件 A 是真的或者条件 B 是真的，那么就执行特定操作。"

条件：
该框显示您为规则提供的所有当前测试条件。点击框中的条件，您可以编辑任意一项。点击紧靠条件旁边的**[Remove]**，您可以删除任意一项。

添加条件
请点击 "添加条件" 来新建一个条件，以便添加到该规则当前的*条件*列表中。添加完条件后，您可通过再次点击该链接来添加更多条件。有关不同类型条件的更多信息，还请参阅下方的规则条件 244。

基于 AI 分类结果的操作：

添加操作
请点击此按钮来打开 AI 分类操作页面，用于指定根据按 AI 模型分配给邮件的分类标签 240，您希望采取什么操作。若选中操作需要更多数据，在此操作下会出现一个相应的控件让您输入该数据。欲获得您可以执行的不同类型操作的信息，请见下方的操作 199。当您为规则设置完所有条件并且选中了一项或更多操作后，请点击 *"保存并关闭"* 来关闭编辑器并在列表中添加新规则。

规则条件

当您希望给一条规则添加一个测试条件时，您将会使用 *"点击此处为该规则添加一个条件"* 链接来打开规则条件这一屏幕。在使用该屏幕来创建测试条件时，您必须首先指定邮件属性，或者您欲进行测试或比较的项目。接着，您必须指定如何测试或比较此项目：该项目是否包含特定文本，它是否完全等同于特定文本，是否存在特定的报头，等等。有若干可被测试的项目，并有多种常见的测试方法。当您已选中项目、测试方法且已输入任何所需信息，请点击 *"保存并关闭"* 从而向您的规则中添加测试条件。

要比较的项目：
这些是您可以在邮件中测试的项目。

- **MAIL (From)** —该测试使用的值就是 SMTP "MAIL From" 命令所通过的值。这就表明了邮件从何而来，不过并不一定要与邮件的 "发件人" 报头所包含的信息完全一致。有时 "发件人" 报头会包含额外信息或者不同信息。除了那九种常见的测试或比较项目的方法之外（见下），该项目同样可以进行比较，使用 "是本地用户" 和 "非本地用户" 测试。
- **RCPT (To)** — 该测试使用的值就是 SMTP "RCPT To" 命令所通过的值。这就表明了邮件从何而来，不过并不一定要与邮件的 "收件人" 报头所包含的信息完全一致。有

时 "收件人"报头会包含额外信息或者不同信息。除了那九种常见的测试或比较项目的方法之外 (见下)，该项目同样可以进行比较，使用 "是本地用户"和 "非本地用户"测试。

- **MAIL and RCPT** —选择此项目来使用 SMTP "MAIL From"和 SMTP "RCPT To"命令来确定邮件是入站、出站还是内部邮件 (请参阅下方的 *"额外测试方法"*)。
- **IP**—选择该项目来测试发件服务器或客户端的 IP 地址。
- **HEADER** — 如果您希望指定一个要比较的报头，请选择该项目。若选中，将出现一个 *"报头名称"*选项，让您指定对于此测试条件，将使用哪个报头。除了那九种常见的测试项目的方法之外，该项目同样可以进行比较，使用 "报头存在"以及 "报头不存在"测试。**注意：**在指定 *"报头名称"*时，在报头名称里不要使用冒号。例如，使用 "发件人"作为 *"报头名称"*，而不用 "发件人："，若您希望比较发件人报头。
- **SUBJECT** —这是邮件的 "主题"报头。若您希望测试邮件的主题，请选择该项目。
- **BODY** — 选择 *"正文"*，若您希望使用邮件正文作为测试项目来比较。
- **BODY or SUBJECT** —在 *"正文"*或 *"主题"*匹配此规则条件时，如果您希望创建一个为 true 的规则，请选择此项目。这个项目是为了简化规则创建而提供的，因为它实际上等同于创建具有两个单独 "OR"语句的规则，一个搜索 *"正文"*，另一个搜索 *"主题"*来查看是否存在相同的文本。
- **ENVIRONMENT (SecurityGateway)** — 如果希望测试条件基于 SecurityGateway 的环境因素，请选择此项，例如：邮件是否来自域邮件服务器 66，发件人是否经过验证，是否位于允许列表 212或阻止列表 205，邮件分值 143是否大于或等于指定的分数，是否邮件被标记为已隔离 (用户) 255或已隔离 (管理员) 256。

如何比较：
此列表中包含了可用来测试或比较项目的方法，这些项目是在 *"上述想比较的对象"*选项里选中的。对于所有项目来说，有多种常见的测试方法。MAIL and RCPT 与 ENVIRONMENT (SecurityGateway) 项目有独特的比较程序集，Mail(From)、RCPT(To) 和 Header 有额外的测试方法。

常见的测试方法：
这些测试方法每一种都是将上述要比较的项目中选中的项目与 *您在下方所指定的如何比较中所选中方法*的搜索值相比较。这些类型的比较都对上方的 *"待比较项目"*选项可用，MAIL、RCPT 和 ENVIRONMENT (SecurityGateway) 除外。他们每个人都有一组独特的比较程序。

- **包含** — 若选中了此方法，如果 *"搜索值"*是一个子字符串或是 *上述指定的要比较项目的一部分*，那么该比较符合条件或者是 "true"。例如，若您选择了 "MAIL (From)"作为要比较的项目，然后选择 "包含"作为比较的方法，以 "example.com"作为 *"搜索值"*，那么来自于含有 "example.com"地址的任意一封邮件都将符合该条件。
- **不包含**—若选中了此方法，如果 *"搜索值"*不是一个子字符串，也不是 *上述指定的要比较项目的一部分*，那么该比较符合条件或者是 "true"。例如，若您选择了 "MAIL (From)"作为要比较的项目，然后选择 "不包含"作为比较的方法，以 "example.com"作为 *"搜索值"*，那么除了那些含有 "example.com"地址的邮件外，其他任意一封邮件都将符合该条件。
- **包含文字** — T此比较器类似于 "包含"，不过仅在字边界锚跟随在此字符串后面时才匹配。这避免了需要手动创建以下格式：\b(word1|word2|word3)\b。例

如：一个规则搜索*包含* "cat"的邮件正文时，只有邮件包含完整的 "cat"时才匹配。如果邮件包含 *catfish* 或 *certificate* 则不匹配。

- **不包含文字**—此比较器类似于 "不包含"，不过仅在不存在含有跟随在此字符串后的字边界锚的字符串时才匹配。例如：一个规则搜索*不包含* "cat"的邮件正文时，将匹配不包含完整 "cat"的任何邮件，即使正文包含 *catfish* 或 *certificate* 时也匹配。
- **等于**—此方法与上述的 *"包含"*类似，不同之处在于 *"搜索值"*必须与 *"要比较项目的值"*完全匹配，而不是仅仅是该值的一部分。例如，若您选择了 IP 作为要比较的项目，然后选择 "等于"作为比较的方法，以 "192.168.0.1"作为 *"搜索值"*，那么只有来自于该准确 IP 地址的邮件才符合条件。
- **不等于**—此类型的比较与先前的方式正好相反。如果 *"要比较项目的值"*与 *"搜索值"不完全相同*，那么该比较是真的。例如，若您选择了 IP 作为要比较的项目，然后选择 "等于"作为比较的方法，以 "192.168.0.1"作为 *"搜索值"*，那么除了那些来自于该准确 IP 地址的邮件外，其他任意一封邮件都符合条件。
- **以...开头**— 当 *"搜索值"*与上述所指定的要比较项目的值开头相符时，*若您希望考虑一个条件为 True*，那么请使用此类型的比较。例如，若您选择 *"主题"*作为要比较的项目，"[allstaff]"作为搜索值，那么所有主题行以 "[allstaff]"开头的邮件都符合条件。
- **不以...开头**—与先前的比较类型正好相反。当 *"搜索值"*与上述所指定的要比较项目的值开头不相符时，*若您希望考虑一个条件为 True*，那么请使用此选项。例如，若您选择 *"主题"*作为要比较的项目，"[allstaff]"作为搜索值，那么除了主题行以 "[allstaff]"开头的邮件以外，其他任意邮件都符合条件。
- **以...结尾**—该比较指的是每当 *"要比较项目的值"*以 *"搜索值"*作为结尾，即符合了条件。例如，若您选择了 RCPT (To) 作为要比较的项目且将 "以...结尾"作为比较方法，以 ".cn"作为搜索值，那么以 ".cn"作为邮件地址结尾的全部邮件都将符合条件。
- **不以...结尾**—该比较指的是每当 *"要比较项目的值"*不以 *"搜索值"*作为结尾，即符合了条件。例如，若您选择了 RCPT (To) 作为要比较的项目且将 "以...结尾"作为比较方法，以 ".cn"作为搜索值，那么除了以 ".cn"作为邮件地址结尾的全部邮件之外，其他任意邮件都将符合条件。
- **匹配正则表达式**—如果您希望在以下情况使用正则表达式，即比较在上方 *"待比较项目"*这一选项中选定的项目，请选择此项。

额外的测试方法：

- **是本地用户**—该比较方法只适用于上述的 MAIL (From) 以及 RCPT (TO) 选项。当邮件地址是本地的 SecurityGateway 用户时，若您希望符合条件或条件为 "true"，请选择此选项。例如，若您选择 MAIL (From) 作为 *"要比较的项目"*，那么只有来自于本地用户的邮件才符合条件。
- **非本地用户**—该比较方法只适用于上述的 MAIL (From) 以及 RCPT (TO) 选项。当邮件地址不是本地的 SecurityGateway 用户时，若您希望符合条件或条件为 "true"，请选择此选项。例如，若您选择 MAIL (From) 作为 *"要比较的项目"*，那么来自于远程用户的所有邮件都符合条件。
- **报头存在**—只有当您选择 "报头"作为 *"要比较的项目"时*，此选项才可用。当您选择了此选项并且在 *"所提供的选项中"*指定了报头的名称，只有当邮件中出现指定报头时才符合条件。例如，若您指定了 "X-我的-自定义-报头"作为 *"报头名称"*，那么所有显示该报头的邮件都符合条件。无此报头的任意一封邮件都不符

合条件。

- **报头不存在**—只有当您选择 "报头"作为 *"要比较的项目"时*，此选项才可用。当您选择了此选项并且在所提供的选项中指定了 *"报头名称"*，只有当邮件中不显示指定报头时才符合条件。例如，若您指定了 "X-我的-自定义-报头"作为 *"报头名称"*，那么所有不显示该报头的邮件都符合条件。显示此报头的任意一封邮件都不符合条件。
- **邮件是/不是 [入站 | 出站 | 内部]**— 这些比较程序仅适用于MAIL and RCPT 项目。SMTP "MAIL From"和 SMTP "RCPT To"值都用于确定邮件是否为入站，出站或内部邮件。
  - **入站**—邮件是指向本地用户的，而不是来自同一个域的本地用户。
  - **出站**—邮件是来自本地用户的，而不是指向同一个域的本地用户。
  - **内部**—邮件来往于同一个域的本地用户。
- **ENVIRONMENT (SecurityGateway) 测试方式** — 以下测试方法仅适用于在您选择了 ENVIRONMENT (SecurityGateway) 作为 *"特比较项目"*的时候：
  - **域邮件服务器** — 该邮件来自或不来自您的域邮件服务器[66]。
  - **已验证发件人**— 选择此项，可根据发件人是否经过身份验证来设置条件。
  - **发件人位于 [允许列表 | 阻止列表]**— 是否是位于允许列表[212]或阻止列表[205]上的发件人。
  - **邮件分值 (大于或等于)**— 使用此项来基于邮件分值[143]设置规则。
  - **已标记邮件：[已隔离 (用户) | 已隔离 (管理员)]**— 按照邮件是否被标记为已隔离 (用户)[255]或已隔离 (管理员)[256]来设置条件。

操作

待为您的规则设置完所有条件后，使用 "规则编辑器"上的 *"操作"*选项来选择当一封邮件符合规则条件时所要执行的操作。有七种操作可供选择：

- **拒收**— 若您希望拒收一封符合该规则内条件的邮件，请选择此操作。当选中了该选项时，在操作下方会出现一个 *"SMTP 反应"*选项，您可以指定在邮件拒收时所发送的文本反应。例如，在 *"SMTP 反应"*选项中，若您使用了，"我们不需要你的垃圾邮件！"，在 SMTP 会话过程中，当 SecurityGateway 拒收一封符合规则的邮件时，它将会发送 "550 我们不要你的垃圾邮件。"
- **删除**—当一封邮件符合规则的条件时，该操作将使邮件被删除。与 "拒收"操作不同的是，该选项不会发送 SMTP 反应，也不会发送投递失败邮件，就单纯地将邮件删除。
- **隔离**—若选中了该操作，如果收件人是本地用户，那么符合该规则下条件的邮件将置于收件人的隔离[255]中。如果收件人是远程用户，那么该邮件将置于管理员隔离[256]中。
- **管理员隔离**—当邮件符合规则下的条件时，若您希望将邮件发送至管理员隔离[256]中，请选择此操作。
- **重定向**—当邮件符合规则下的条件时，使用该操作，将邮件重定向至其他地址。在

操作下提供了一个 *"收件人"*选项，这样您便可指定将邮件重定向至哪个邮件地址。重定向的邮件将不会发送至初始收件人...邮件被重新路由至该操作中指定的地址。

- **复制**—若您希望将邮件复制到一个额外的邮件地址，请使用此选项。在操作下提供了一个 *"收件人"*选项，这样您便可指定将邮件发送至哪个邮件地址。与 "重定向"类似，不同之处在于在复制操作中，初始收件人以及此操作所指定的地址都将受到该邮件的副本。若您希望将一封邮件复制到多个地址，那么您可为每个地址指定一条额外的规则。
- **发送提示 (警告)**—当一封邮件符合规则下条件时，若希望向某人发送一封提示或者警告邮件，请使用此操作。若选中了此操作，会向您提供选项以指定提示的*收件人*、*发件人*、*主题*以及*邮件文本* (邮件的正文)。在提示中您可使用一些宏，从而动态地包含一些特定信息。当 SecurityGateway 碰到带宏的提示文本，它会用相应的值将其取代。可使用以下宏：

  $发件人$—以用于符合规则邮件的 SMTP MAIL From 地址来取代。例如，"sender@example.net"。

  $发件人邮箱$—该宏仅仅是以通过 SMTP MAIL From 命令的邮件地址的邮箱部分来取代。例如，"sender@example.net"地址中的 "sender"。

  $发件人域$—该宏仅仅是以通过 SMTP MAIL From 命令的邮件地址的域部分来取代。例如，"sender@example.net"地址中的 "example.net"。

  $收件人$—以用于符合规则邮件的 SMTP RCPT To 地址来取代。例如，"recipient@example.com"..

  $收件人邮箱$—该宏仅仅是以通过 SMTP RCPT To 命令的邮件地址的邮箱部分来取代。例如，"recipient@example.com"地址中的 "recipient"。

  $收件人域$—该宏仅仅是以通过 SMTP RCPT To 命令的邮件地址的域部分来取代。例如，"recipient@example.com"地址中的 "example.com"。

  $主题$该宏是以符合条件的邮件 "主题"报头的内容来取代。

  $邮件 ID$—该宏是以邮件的 "邮件 ID"报头之值来取代。

  $日期戳$—该宏是以邮件的日期来取代。

  $当前时间$— 该宏是以 SecurityGateway 创建提示的当前时间来取代。

  $HELO 名称$— 这是当 SecurityGateway 收到符合规则的邮件时，在 SMTP 会话过程中所通过的 HELO 域。

- **添加到邮件分值**—如果您希望在邮件符合规则条件时，为邮件评分添加特定数量的分数，请使用此操作。
- **发送为已注册邮件 (RMail)**—如果您希望在邮件符合规则条件时使用 RMail 的 Registered Email (注册邮件)功能中的一项或多项，请使用此操作。

  加密—果要加密邮件，请选择此选项。

  跟踪 & 证明—如果使用 RMail 的跟踪和证明功能，请选择此选项。

  电子签名—如果您希望使用 RMail 的电子签名功能进行电子签名文件，请选择此选项。

- **为 REQUIRETLS 标记邮件**—指示该邮件应使用 RequireTLS。

- **发送为安全 web 邮件**—如果您希望使用 SecurityGateway 的安全通信[90] web 门户系统来发送邮件，而不是使用传统的邮件投递，请选择此操作。
- **添加报头** — 这是 AI 分类[243]规则操作，您可以使用该操作来将报头添加到匹配了规则条件的邮件中。指定报头名称，然后选择您是否希望报头值是邮件分类标签[240]的报头，还是您提供的自定义值。
- **标记主题报头** — 这是 AI 分类[243]规则操作，您可以用来将标签添加到邮件主题报头。您可以选择标签是否是邮件的分类标签[240]还是您提供的自定义值。

正则表达式

规则条件[196]支持 "匹配正则表达式"作为比较方法。正则表达式 (regexp)是一个功能全面的系统，不仅帮助您搜索特定的文本字符，也可以搜索到文本类型。一个正则表达式的文本类型包含特殊字符的组合，成为 *"元字符"*以及字母数字文本字符，或者 *"文字"* (例如：abc，123，等等)。该类型用于匹配文本字符— 并附有匹配的结果，是成功还是失败。

SecurityGateway 的正则表达式方案使用的是 PERL 兼容性正则表达式 (PCRE)库。您可以在此获得正则表达式方案的更多信息：http://www.pcre.org/ 和 http://perldoc.perl.org/perlre.html。

如果要对正则表达式有一个全面的了解，请参阅：*掌握正则表达式，第三版* 由 O'Reilly Media, Inc.出版。

元字符

在正则表达式中，元字符是有特定功能及用途的特殊字符。在 SecurityGateway 中的正则表达式方案可允许使用下列元字符：

\ | () [] ^ $ * + ? .

元字符	描述
\	若在一元字符钱使用反斜线 ("\")，将使元字符被处理为文字字符。若您希望正则表达式搜索其中一个用作元字符的特殊字符，这一点是有必要的。例如，要搜索 "+"您的表达式中必须包含 "\+"。
|	使用*交替*字符 (亦叫做 *"或"*或者 *"竖线"*)，当您希望字符两侧的其中一个表达式符合目标字符。正则表达式是 "abc|xyz"。搜索一个文本字符时，会出现符合条件的 "abc"或 "xyz"。
[...]	框 ("[" 及 "]")内包含的字符组就表示该组中的任意字符都可能符合所查找的文本字符。括号里字符间的破折号 ("-")表示了字符的范围。例如，在表达式 "[a-z]"中搜索字符 "abc"将生成三个匹配项：*"a,"* *"b,"*以及 *"c。"*使用表达式 "[az]"只会生成一个匹配项：*"a。"*

^	表示字符串的开头。在目标字符串中，“abc ab a”表达式“^a”将生成一个匹配项—目标字符串中的第一个字符。正则表达式“^ab”也将生成一个匹配项—*目标字符串中的*第一第二个字符。
[^...]	紧跟左括号（“[”）后的插入记号（“^”）有不同的含义。用于将括号内剩余的字符排除在符合条件的目标字符串之外。表达式“[^0-9]”表明目标字符不是数字。
(...)	圆括号影响了样式估计的顺序，也可作为*带标记的*表达式，用于*搜索和替换*表达式。 正则表达式的搜索结果可以暂时保存，也可用于*替换*表达式以建立新的表达式。在*替换*表达式中，您可以包含一个“&”或者“\0”字符，将会以正则表达式搜索过程中所找到的子字符串来替换。所以，如果*搜索*表达式“a(bcd)e”找到了一个子字符串匹配项，那么“123-&-123”或者“123-\0-123”的替换*替换*表达式将以“123-abcde-123”来替换符合条件的文本。 同样地，在替换表达式中您也可以使用特殊字符“\1,”“\2,”“\3,”*等等*。这些字符只会被*已标记*表达式的结果所替代，而不是整个子字符串的匹配项。紧跟反斜线的数字表明您想要引用的带标记表达式（如果正则表达式中包含了不知一个带标记的表达式）。例如，如果您的*搜索*表达式是“(123)(456)”并且您的*替换*表达式是“a-\2-b-\1”，那么一个符合的自字符将由“a-456-b-123”替代，而“a-\0-b”的一个*替换*表达式将以“a-123456-b”替代。
$	美元记号（“$”）代表字符串的结尾。在文本字符串中，“13 321 123”表达式“3$”将生成一个匹配项—字符串中的最后一个字符。正则表达式“123$”也将生成一个匹配项——*目标字符串中的*最后三个字符。
*	星号（“*”）量词表明星号左边的字符*在一行字符中出现的次数*必须大于等于零次。那么“1*abc”将符合文本“111abc”以及“abc”。
+	与星号量词类似，“+”量词表明加号左边的字符*在一行字符中出现的次数*必须大于等于一次。那么，“1+abc”将符合文本“111abc”而不符合文本“abc”。
?	问号（“?”）量词表明问号左边的字符必须符合*零或*一次。那么，“1*abc”将符合文本“abc”，并且符合“111abc”的“1abc”部分。
.	句号或者点（“.”）元字符将符合任何其他字符。那么“.+abc”将符合“123456abc”，且“a.c”将符

	合“ac”，“abc”，“acc”等等。

章节

6

6 邮件/队列

左窗格的邮件/队列菜单选项帮助您访问以下两个部分：邮件日志与邮件队列。

邮件日志

邮件日志针对您用户发送与接收的每封邮件，都会包含一个条目。它列出了邮件的处理日期和时间，发件人和收件人，以及邮件主题。此外，还列出了投递结果，如是否被投递、隔离或拒绝，若未投递还会提供原因，如发件人被列入阻止列表，邮件包含受限制的附件等等。最后，每个条目还会列出邮件的大小与其邮件总值143。

根据邮件日志，您可以查看每封邮件的详情，包括其投递的记录和邮件的内容与总值（可用时）。您还可以将邮件标记为垃圾邮件或非垃圾邮件，这有助于改进 SecurityGateway 的贝叶斯学习131功能并且更准确的对邮件进行分类。

> 邮件日志同样可以在日志260菜单中获得。

邮件队列

这部分提供了链接，通往四个不同的邮件队列：用户隔离区255、管理隔离区256、邮件等待投递队列257、与坏邮件258。

- 用户隔离区255是一个保持队列，当一个指定的功能被配置为将投递失败的邮件隔离，而不是拒收或为它们添加标签的时候，会用于没有通过 SecurityGateway 各种安全124功能的接收邮件。用户可以登陆到 SecurityGateway 查看他们隔离文件夹的内容，并从中选择以查看邮件，删除邮件或为它们解除隔离状态以便进行正常投递。
- 管理隔离区256与用户隔离区类似，但是它针对的是外发邮件与含有病毒的邮件。只有管理员50才能访问管理隔离区。
- 等待投递队列257是一个队列，针对所有等待投递的邮件，包括那些无法投递的邮件与当前处于重试系统76的邮件。您可以从该页查看队列中的任何邮件，将邮件退回至其发件人，停止邮件的投递，或者立即重试投递队列中的一封选中邮件或所有邮件。
- 坏邮件258队列是针对那些因为发生致命处理错误而无法进行投递的邮件，比如一封邮件在递归循环中被捕获，使之达到*最大邮件跳跃计数*78。您可以从坏邮件队列查看队列中的任何邮件，可以设法将邮件退回至其发件人，删除邮件，或者立即重试投递队列中的一封选中邮件或所有邮件。

6.1 所有邮件

点击“**所有邮件**”来显示“邮件”日志。邮件日志针对您用户发送与接收的每封邮件，都会包含一个条目。它列出了邮件的处理日期和时间，发件人和收件人，以及邮件主题。此外，还列出了投递结果，如是否被投递、隔离或拒绝，若未投递还会提供原因，如发件人被

列入阻止列表，邮件包含受限制的附件等等。最后，每个条目还会列出邮件的大小与其邮件总值 143。

在邮件日志页面顶部的工具栏上有数个按钮，可用于执行以下任务：

- **刷新**—点击该按钮刷新邮件日志，以显示自您开始查看日志以来可能新增的条目。
- **搜索**—使用丰富的搜索功能来过滤邮件日志，以便只显示特定邮件。可基于是入站邮件还是出站邮件来搜索日志，搜索报头中的特定文本，搜索所有日期或日期起至范围等等。要搜索邮件日志：请点击 工具栏上的 *"搜索"*按钮以打开搜索窗口，然后选择搜索条件，最后点击该窗口内的*搜索*按钮执行搜索。 "搜索"窗口将被隐藏，搜索结果将出现在 "邮件日志"中。再次点击 *"显示搜索"*来修改该搜索，或点击 *"取消搜索"*来取消该搜索并将 "邮件日志"返回到常规状态。
- **详细信息**—选择一封邮件，然后点击此按钮 (或双击该邮件)来打开 **"邮件信息"**屏幕。该屏幕有三个选项卡：记录、邮件和来源。 "记录"选项卡包含投递过程的记录，包括 SMTP 会话和内部处理等。 "邮件"选项卡包含邮件的实际内容，并提供用来下载邮件及其附件的选项。该选项卡的可行度取决于邮件的存在时间长短，邮件是否投递成功，还有位于数据保留 116页面的哪些选项处于激活状态。来源选项卡包含邮件的来源，其中包括邮件的报头、html代码等。如果邮件过旧或者并没有将 SecurityGateway 的数据保留 116选项设置成保存该信息，那么来源选项卡可能不可用。
- **重新投递**—选择该列表中的一封或多封邮件，然后点击此按钮将其重新投递至收件人。使用 Ctrl+Click 或 Shift+Click 以选择多封邮件。仅当邮件内容尚未从数据库中删除时，才能使用该选项。
- **垃圾邮件**—选择一则邮件并单击该按钮将邮件标记为垃圾邮件。这可帮助 SecurityGateway 以后更为精确地识别垃圾邮件。禁用贝叶斯 131功能时，该选项将不可用。
- **非垃圾邮件**—选择一则邮件并点击该按钮将邮件标记为非垃圾邮件。这有助于防止 SecurityGateway 以后错误地将合法邮件标识为垃圾邮件。禁用贝叶斯 131功能时，该选项将不可用。
- **允许列表/阻止列表**—选择一封邮件并点击允许列表 213或阻止列表 205。然后点击要添加发件人或发件人域的地址列表：用户列表、域列表或全局列表。

6.2 邮件队列

6.2.1 隔离（用户）

用户隔离区是一个保持队列，针对没有通过 SecurityGateway 各种安全 124功能的接收邮件提供了一种方法，凭此保护您的邮件服务器与用户免于接收大量涌入的垃圾邮件与其他可疑的或有害的邮件。SecurityGateway 的大多数安全功能提供了一个选项，可以隔离满足某种条件的邮件，而不是进行删除或者为它们添加标签。用户隔离区中的邮件会保留在 SecurityGateway 里，收件人或管理员可以于此管理这些邮件。——用户可以登陆并查看他们隔离文件夹的内容，还可以从中选择以查看邮件，删除邮件或为它们解除隔离状态以便进行正常投递。

被隔离的外发邮件与含有病毒的邮件将会保留在管理隔离区[256]中。只有管理员[50]才能访问那些邮件。

隔离区的每一条目分成数列，分别列出了邮件被隔离的日期和时间、发件人、收件人以及主题等。还有一些列显示邮件被隔离的原因，邮件大小与其邮件总值[143]。

在隔离区页面顶部的工具栏上有数个按钮，可用于执行以下任务：

- **刷新**—点击该按钮刷新隔离区，以显示自您开始查看隔离区以来可能新增的邮件。
- **搜索**——使用丰富的搜索功能过滤用户隔离区以仅仅显示指定的邮件。您可以根据邮件是接收的还是外发的来进行搜索，搜索任何报头内的指定文本，搜索所有或者一系列的数据等等。要搜索隔离区：点击工具栏上的*"搜索"*按钮以打开搜索窗口，然后选择搜索条件，最后点击该窗口内的搜索按钮执行搜索。搜索结果会出现在搜索窗口下方—过滤隔离区以便只显示匹配搜索参数的邮件。要隐藏搜索窗口同时保留下方的过滤结果，可在工具栏上再次点击*"搜索"*。完成您的搜索之后，请点击搜索窗口中的*"取消"*将用户隔离区复原为标准状态。
- **查看**—选择一则邮件，然后点击该按钮可打开邮件信息屏幕。该屏幕有三个选项卡：记录、邮件和来源。记录选项卡包含了邮件投递过程的记录，包括 SMTP 会话，内部处理等等。邮件选项卡包含邮件的实际内容，来源选项卡包含邮件的来源，其中包括邮件报头、html代码等。
- **释放**—选择一则邮件，然后点击该按钮从隔离区将其释放以进行投递。
- **删除**—选择一则邮件并点击该按钮将其删除。
- **全部删除**—点击该按钮删除全部隔离邮件。

6.2.2 隔离（管理员）

管理隔离区与用户隔离区[255]类似。但是，当一个指定的功能被配置为将投递失败的邮件隔离，而不是拒收或为它们添加标签的时候，管理隔离区针对的是接收邮件，而不是含有病毒的邮件与没有通过 SecurityGateway 各种安全[124]功能的外发邮件。不像用户隔离区，在管理隔离区中只有管理员才能访问邮件。管理员可以查看邮件，删除邮件，或者为它们解除隔离状态以进行正常的投递。

管理隔离区中的每个条目都具有一列会列出邮件被隔离的日期与时间，有一些列用于显示发件人，收件人与邮件主题。还有一些列显示邮件被隔离的原因，邮件大小与其邮件总值[143]。

管理隔离区顶部的工具栏中有一些按钮，您可以使用这些按钮来执行许多任务：

- **刷新**——点击该按钮刷新被隔离的邮件列表，以显示自您进入该页面起可能已被添加的邮件。
- **搜索**——使用丰富的搜索功能过滤管理隔离区以仅仅显示指定的邮件。您可以根据邮件是接收的还是外发的来进行搜索，搜索任何报头内的指定文本，搜索所有或者一系列的数据等等。要搜索管理隔离区：点击工具栏上的*"搜索"*按钮以打开搜索窗

口，然后选择搜索条件，最后点击该窗口内的搜索按钮执行搜索。搜索结果将在搜索窗口下显示——将过滤管理隔离区以仅显示与搜索参数匹配的邮件。要隐藏搜索窗口同时保留下方的过滤结果，可在工具栏上再次点击 *"搜索"*。搜索执行完毕，在搜索窗口内点击 *"取消"*使隔离区页面恢复常态。

- **查看**—选择一则邮件，然后点击该按钮可打开邮件信息屏幕。该屏幕有三个选项卡：记录、邮件和来源。记录选项卡包含了邮件投递过程的记录，包括 SMTP 会话，内部处理等等。邮件选项卡包含邮件的实际内容，来源选项卡包含邮件的来源，其中包括邮件报头、html代码等。
- **释放**—选择一则邮件，然后点击该按钮从隔离区将其释放以进行投递。
- **删除**—选择一则邮件并点击该按钮将其删除。
- **全部删除**—点击该按钮删除全部隔离邮件。

6.2.3 排队等待投递

等待投递队列是一个队列，用于所有将至或来自某个远程地址的与等待着被投递的邮件，包括那些无法投递与当前正处于重试系统[76]中的邮件。您可以从该页查看队列中的任何邮件，将邮件退回至其发件人，停止邮件的投递，或者立即重试投递队列中的一封选中邮件或所有邮件。"排队等待发送"列表中的每个条目都会显示邮件是入站还是出站邮件，列中列出收到邮件的日期和时间、并且具有发件人、收件人、主题和邮件大小的列、以及投递尝试结果的列。

等待投递队列列表顶部的工具栏中有一些按钮，您可以使用这些按钮来执行许多任务：

- **刷新**——点击该按钮刷新排队邮件列表，以显示从您进入该页面起可能已被添加的邮件。
- **搜索**——使用丰富的搜索功能过滤列表以仅仅显示指定的邮件。您可以根据邮件是接收的还是外发的来进行搜索，搜索任何报头内的指定文本，搜索所有或者一系列的数据等等。要搜索等待投递队列列表：点击工具栏上的 *"搜索"*按钮以打开搜索窗口，然后选择搜索条件，最后点击该窗口内的搜索按钮执行搜索。搜索结果将在搜索窗口下显示——将过滤等待投递队列列表以仅显示与搜索参数匹配的邮件。要隐藏搜索窗口同时保留下方的过滤结果，可在工具栏上再次点击 *"搜索"*。完成您的搜索之后，请点击搜索窗口中的 *"取消"*将该列表复原为标准状态。
- **查看**—选择一则邮件，然后点击该按钮可打开邮件信息屏幕。该屏幕有三个选项卡：记录、邮件和来源。记录选项卡包含了邮件投递过程的记录，包括 SMTP 会话，内部处理等等。邮件选项卡包含邮件的实际内容，来源选项卡包含邮件的来源，其中包括邮件报头、html代码等。
- **退回**——选中一封邮件并点击该按钮以将该邮件返回，或"退回"给发件人。这将会停止尝试将邮件投递至其目标收件人。
- **停止投递**——选中一封或多封排队邮件并单击该按钮以将邮件的状态更改为"投递失败"，这样就能阻止邮件发送。但是，如果一封邮件在单击该按钮时已处于投递过程，将无法停止此邮件的发送。
- **全部停止**——与以上的*停止投递*功能类似，唯一不同处在于该功能应用于队列中的所有邮件。如果使用搜索功能过滤列表，则只有列表中显示的那些邮件将被停止。

- **重试投递**——选中队列中的一封邮件并单击该按钮以让 SecurityGateway 立即重试投递此邮件，而不是等待下一个重试周期[76]。
- **全部重试**——点击该按钮以让 SecurityGateway 立即尝试投递所有的排队邮件，而不是等待每一封邮件的下一个重试周期[76]。

6.2.4 坏邮件

坏邮件[258]队列是针对那些因为发生致命处理错误而无法进行投递的邮件，比如一封邮件在递归循环中被捕获，使之达到最大邮件跳跃计数[78]。您可以从坏邮件队列查看队列中的任何邮件，可以设法将邮件退回至其发件人，删除邮件，或者立即重试投递队列中的一封选中邮件或所有邮件。坏邮件列表中的各个条目显示了该邮件是接收还是外发的，条目中有一列列出了接收邮件的日期与时间，还有一些列用于邮件的发件人，收件人，主题与大小。

坏邮件列表顶部的工具栏中有一些按钮，您可以使用这些按钮来执行许多任务：

- **刷新**——点击该按钮刷新邮件列表，以显示自您进入该页面起可能已被添加的邮件。
- **搜索**——使用丰富的搜索功能过滤列表以仅仅显示指定的邮件。您可以根据邮件是接收的还是外发的来进行搜索，搜索任何报头内的指定文本，搜索所有或者一系列的数据等等。搜索坏邮件列表：点击工具栏上的 *"搜索"*按钮以打开搜索窗口，然后选择搜索条件，最后点击该窗口内的搜索按钮执行搜索。搜索结果将在搜索窗口下显示——将过滤坏邮件列表以仅显示与搜索参数匹配的邮件。要隐藏搜索窗口同时保留下方的过滤结果，可在工具栏上再次点击 *"搜索"*。完成您的搜索之后，请点击搜索窗口中的 *"取消"*来将邮件列表复原为标准状态。
- **查看**—选择一则邮件，然后点击该按钮可打开邮件信息屏幕。该屏幕有三个选项卡：记录、邮件和来源。记录选项卡包含了邮件投递过程的记录，包括 SMTP 会话，内部处理等等。邮件选项卡包含邮件的实际内容，来源选项卡包含邮件的来源，其中包括邮件报头、html代码等。
- **退回**——选中一封邮件并单击该按钮以尝试将该邮件返回，或 "退回"给发件人。
- **删除**——选中一封邮件并点击该按钮以将该邮件从坏邮件队列中删除。使用 "删除"按钮下拉列表选择仅删除所选邮件或删除列表中的所有邮件。
- **重试投递**——在队列中选中一封邮件并单击该按钮以让 SecurityGateway 再次尝试投递该邮件。这会将邮件移至等待投递队列[257]页面。如果修正了引起邮件投递终止并被置于坏邮件队列的错误，那么投递就可能成功。否则邮件可能再次投递失败并被置回坏邮件队列。
- **全部重试**——单击该按钮以让 SecurityGateway 重新尝试投递所有包含在坏邮件队列中的邮件。如果您修正了一些引起邮件被置于队列中的错误，这是很有帮助的。

章节

7 日志

左窗格的日志菜单选项帮助您访问以下三部分：邮件日志，日志文件与配置

邮件日志 254

邮件日志针对您用户发送与接收的每封邮件，都会包含一个条目。它列出了邮件的处理日期和时间，发件人和收件人，以及邮件主题。此外，还列出了投递结果，如是否被投递、隔离或拒绝，若未投递还会提供原因，如发件人被列入阻止列表，邮件包含受限制的附件等等。最后，每个条目还会列出邮件的大小与其邮件总值 143。

根据邮件日志，您可以查看每封邮件的详情，包括其投递的记录和邮件的内容与总值（可用时）。您还可以将邮件标记为垃圾邮件或非垃圾邮件，这有助于改进 SecurityGateway 的贝叶斯学习 131功能并且更准确的对邮件进行分类。

> 邮件日志同样可以从邮件/队列 254菜单抵达。

日志文件 261

您可以使用日志文件部分来查看 SecurityGateway 保存在您日志文件夹 109中的各种日志文件。不像邮件日志，日志文件并不贮存在数据库中，也不向每种事件提供可保存的列表与独立的条目。取而代之的，它们只是纯文本文件，记录各种 SMTP 连接与其他 SecurityGateway 执行的功能。所有日志文件的页面位于日志文件部分之下，列出了包含在您日志文件夹中的所有日志文件，包括当前的日志文件与翻转 262日志文件。您可以从那页面查看所有列出的文件。日志文件部分的其他页面提供了可以查看 SecurityGateway 当前日志文件的快捷方式，例如系统日志、接收与外发日志、病毒库更新日志等等。

配置 262

配置部分提供了一条链接，通往日志配置 262页面，用于配置您日志的首选项与选项。在该页您可以根据您的需要指定在接收，发送与 HTTP 日志中，那些将写入的数据的详细程度。您还可以选择将被创建的日志文件的类型。标准设置，每天一个新设置且将日期并入文件名，或者每天一个新设置且将星期几并入文件名。最后，您可以选择各种日志文件维护设置，比如在保存文件前与新建文件前的大小规定，可以创建的“翻转”文件的数量，文件在归档前可以存在的时间长短等等。

7.1 所有邮件

点击“**所有邮件**”来显示“邮件”日志。邮件日志针对您用户发送与接收的每封邮件，都会包含一个条目。它列出了邮件的处理日期和时间，发件人和收件人，以及邮件主题。此外，还列出了投递结果，如是否被投递、隔离或拒绝，若未投递还会提供原因，如发件人被列入阻止列表，邮件包含受限制的附件等等。最后，每个条目还会列出邮件的大小与其邮件总值 143。

在邮件日志页面顶部的工具栏上有数个按钮，可用于执行以下任务：

- **刷新**—点击该按钮刷新邮件日志，以显示自您开始查看日志以来可能新增的条目。
- **搜索**—使用丰富的搜索功能来过滤邮件日志，以便只显示特定邮件。可基于是入站邮件还是出站邮件来搜索日志，搜索报头中的特定文本，搜索所有日期或日期起至范围等等。要搜索邮件日志：请点击 工具栏上的 *"搜索"*按钮以打开搜索窗口，然后选择搜索条件，最后点击该窗口内的*搜索*按钮执行搜索。 "搜索"窗口将被隐藏，搜索结果将出现在 "邮件日志"中。再次点击 *"显示搜索"*来修改该搜索，或点击 *"取消搜索"*来取消该搜索并将 "邮件日志"返回到常规状态。
- **详细信息**—选择一封邮件，然后点击此按钮 (或双击该邮件)来打开 **"邮件信息"**屏幕。该屏幕有三个选项卡：记录、邮件和来源。 "记录"选项卡包含投递过程的记录，包括 SMTP 会话和内部处理等。 "邮件"选项卡包含邮件的实际内容，并提供用来下载邮件及其附件的选项。该选项卡的可行度取决于邮件的存在时间长短，邮件是否投递成功，还有位于数据保留[116]页面的哪些选项处于激活状态。来源选项卡包含邮件的来源，其中包括邮件的报头、html代码等。如果邮件过旧或者并没有将 SecurityGateway 的数据保留[116]选项设置成保存该信息，那么来源选项卡可能不可用。
- **重新投递**—选择该列表中的一封或多封邮件，然后点击此按钮将其重新投递至收件人。使用 Ctrl+Click 或 Shift+Click 以选择多封邮件。仅当邮件内容尚未从数据库中删除时，才能使用该选项。
- **垃圾邮件**—选择一则邮件并单击该按钮将邮件标记为垃圾邮件。这可帮助 SecurityGateway 以后更为精确地识别垃圾邮件。禁用贝叶斯[131]功能时，该选项将不可用。
- **非垃圾邮件**—选择一则邮件并点击该按钮将邮件标记为非垃圾邮件。这有助于防止 SecurityGateway 以后错误地将合法邮件标识为垃圾邮件。禁用贝叶斯[131]功能时，该选项将不可用。
- **允许列表/阻止列表**—选择一封邮件并点击允许列表[213]或阻止列表[205]。然后点击要添加发件人或发件人域的地址列表：用户列表、域列表或全局列表。

7.2 日志文件

您可以使用日志文件部分来查看 SecurityGateway 保存在您日志文件夹[109]中的各种日志文件。不像邮件日志，日志文件并不贮存在数据库中，也不向每种事件提供可保存的列表与独立的条目。取而代之的，它们只是纯文本文件，记录各种 SMTP 连接与其他 SecurityGateway 执行的功能。所有日志文件的页面位于日志文件部分之下，列出了包含在您日志文件夹中的所有日志文件，包括当前的日志文件与翻转[262]日志文件。您可以从那页面查看所有列出的文件。日志文件部分的其他页面提供了可以查看 SecurityGateway 当前日志文件的快捷方式，例如系统日志、接收与外发日志、病毒库更新日志等等。

使用 SecurityGateway 的内部备份[118]选项创建的备份文件并不包括日志文件。但是您可以使用位于日志配置[262]页面上的归档选项对日志文件进行归档。如果您希望将日志文件保存或备份在一

> 个其他的位置，而不是指定的日志[109]目录中，那么您就必须使用您的备份软件或者一些外部方法来实现这一点。

所有日志文件

所有日志文件的页面列出了所有包含在您日志文件夹中的日志文件，均被指定在目录[109]页面。它列出了那些仍被 SecurityGateway 不断写入的当前文件与翻转[262]日志文件。每个条目列出了文件名，文件大小以及其最后被修改的日期与时间。您可以查看任何列出的文件，只要双击其条目或者选中该条目并单击位于此页顶部工具栏中的 *"查看"*。您可以下载文件，只要选中该文件并单击下载按钮。您可以删除文件，只要选中该文件并点击删除按钮。

当前日志

日志文件部分中剩下的链接将您直接带到 SecurityGateway 正在使用中的当前文件。有直接的链接，可查看以下的当前日志文件：

- **系统**——系统日志用于以下事件，例如 SecurityGateway 服务的启动与停止、SMTP、SSL、HTTP 和其他服务的初始化，某些系统错误等。
- **入站**——SecurityGateway 的入站日志包含了针对所有入站邮件的会话记录。
- **出站**——该日志包含了针对所有出站邮件的会话记录。
- **路由**——路由日志列出了相关于发送至您用户与服务器的 SecurityGateway 路由邮件在被接收之后的所有活动。
- **变更**—变更日志列出了对 SecurityGateway 配置的所有变更，以及进行更改的人员。
- **归档**—该日志包含相关归档[85]的所有活动。
- **POP**—此日志包含与任何已配置的 POP 账户[68]相关的任何活动的记录。
- **HTTP**——该日志包含了所有与 HTTP 相关的数据与行为。
- **ClamAV 更新**——ClamAV 更新日志文件列出了关于您 ClamAV 病毒特征的更新情况。
- **IKARUS Anti-Virus 日志**—有三个日志文件与 IKARUS 病毒签名更新、引擎状态和扫描有关。

7.3 配置日志

日志配置是用来配置您日志的首选项与选项的。要抵达日志配置页面，请点击位于左窗格里的 *"日志»配置»配置日志"*。在该页您可以根据您的需要指定在接收，发送与 HTTP 日志中，那些将写入的数据的详细程度。您还可以选择将被创建的日志文件的类型。标准设置，每天一个新设置且将日期并入文件名，或者每天一个新设置且将星期几并入文件名。此外，您可以选择各种日志文件维护设置，比如文件在保存前与新文件创建前的大小规定，可以创建的 "翻转"文件的数量，文件在归档前可以存在的时间长短等等。所有的日志文件保存在指定在目录[109]页面的日志文件夹中。

日志级别

这部分选中的选项控制了入站 SMTP，出站 SMTP 与 HTTP 日志文件[261]的大小。该设置将不会影响系统，路由与其他日志文件。

调试
这是一个最为详细的用于接收，外发与 HTTP 日志文件的日志选项。因为这个选项会产生大型的日志文件，在执行时会带来负面影响，所以一般情况下，不应该选择这个方法处理日志。不过在尝试调试一个问题时，这个方法将很有帮助。

信息
这是默认的选项，在大多数情况下推荐使用该设置。日志并不像以上的调试选项这般扩展，但仍会针对成功与失败的事件创建日志条目。

警告
如果您仅希望记录失败的事件与其他潜在的问题，请选择该选项。

错误
选中该选项时，仅会记录失败的事件。选择这个日志级别会提高性能。

无
如果您不希望记录任何接收，外发或 HTTP 事件，请选择该选项。不推荐使用该选项。

日志模式

这部分你所选择的选项控制了用于日志文件的命名转换。

创建一套标准的日志文件
选中该项时，SecurityGateway 将产生一套使用命名方案的标准日志文件。SecurityGateway-Inbound.log, SecurityGateway-Outbound.log, SecurityGateway-System.log, 等等。

每天创建一套新的日志文件
这是默认选项。该选项在每个午夜创建一套新的日志文件。日期已并入每个文件的名字当中。例如：SecurityGateway-20080315-Inbound.log 针对入站 SMTP 日志文件，该文件于2008年3月15日创建而成。

在日志文件名中包含计算机名称
如果您希望在日志文件名中包含计算机名，请启用此选项。如果日志文件夹被设置成 UNC 路径，则此项为必要选项，而且它允许一个集群[111]中的多个服务器记录到同一个位置。

不记录来自这些 IP 地址的 SMTP 或 HTTP 连接
使用此选项，可以指定您不希望为其记录 SMTP 或 HTTP 连接的任何 IP 地址。来自指定 IP 地址的不完整和拒绝的 SMTP 邮件也不会添加到数据库中。如果邮件被接受进而投递，它将被添加到数据库中。

日志维护

这部分的选项控制了日志文件的大小，翻转日志文件所允许的数量，是否将覆盖现有的日志文件，以及归档旧日志文件的频率。

最大日志文件大小：[xx]KB （0＝大小不限）
使用该选项来指定任何日志所允许的最大规格（以 KB 计算）。当文件达到这个最大规格，它将被重命名为*.OLD并启动一个新文件。"翻转"文件所允许的数量是由以下的*日志翻转文件的最大数量*选项决定的。

日志翻转文件的最大数量：
该选项控制了每个日志文件所允许的翻转文件的数量。当日志文件达到以上指定的*"最大日志文件大小"*，就会产生一个新的翻转文件。这些文件使用以下命名方案："filename(1).old"，"filename(2).old"，"filename(3).old"等等。每一次有新的翻转文件产生的时候，其他所有的翻转文件都会被重命名，这样最新的数据总是处于第一个文件。例如，"filename(1).old"总是作为最新的翻转文件，"filename(2).old"将作为第二个最新的文件，以次类推。当达到文件的最大数量时，将会删除最旧的文件，而其余的文件仍会照常进行重命名。该选项的默认值是 10。

当日志文件名在午夜变更时，覆盖现有日志文件
当选中了以上的*"根据星期几来创建日志文件"*选项时，每晚午夜 SecurityGateway 将创建一套新的日志文件，并将星期几并入每个文件名。在创建时，该选项决定了是否覆盖现有的重名文件，还是让 SecurityGateway 将新的数据附加至旧文件的末尾。例如，如果启用该选项，且在周日 SecurityGateway 发现"SecurityGateway-Sunday-Inbound.log"文件已经存在，那么该文件就会被覆盖，仅当天的信息会包含其中。如果禁用该选项，那么所有当天的数据将被附加至现有文件的末尾。默认情况下，禁用该选项。

自动 ZIP 并归档日志文件存在时间大于：[xx]天 （0=从不）
每晚午夜，SecurityGateway 将对所有存在时间大于该选项指定天数的日志文件进行压缩与移动。该天数存在于"\日志\旧日志\ 目录[109]"中。该选项的默认值是 14。

章节

8

8 报告

报告部分提供了互动而详尽的关于 SecurityGateway 行为的图表报告。您可以产生显示接收邮件数量较之外发邮件数量的报告，对接收的垃圾邮件类型进行分析的报告，带宽的报告，根据累积邮件大小而排出的顶级发件人的报告，病毒报告等等。此外，每个报告还提供选项，允许您指定报告的参数。比如，您可以指定报告中的数据用于特定的域或所有的域；按小时、天数，月数来数绘制数据；报告的数据采集还包括了固定的时间周期，比如一天、一周、一个月或使用一段您指定的日期。不仅如此，每个报告之下还有一个细目表，对报告内容作了分析，还提供了链接通往邮件日志 260，日志将被过滤以显示仅与报告中的该条目相关的数据。比如，它提供了链接以显示在指定的小时内列在报告上的所有接收邮件，在某一天收到的所有包含病毒的邮件，一个域中的顶级收件人收到的所有邮件等等。为报告选定参数之后，只要单击位于该页顶部工具栏上的 *"查看"*就可使用该条件产生一份新报告。

"报告"菜单下有六部分：

调度报告

这部分包含统计报告选项：

- **统计报告**—这是一个通用的统计报告，可用于快速确定服务器的状态和过滤效果。它可以每晚或每周发送给全局管理员，域管理员和手动定义的电子邮件地址列表。对于域管理员，该报告仅包含域（该管理员对此域具有管理权限）的统计信息。

  在"统计报告"屏幕上，请选择"调度"屏幕中的 *午夜*或 *每周*来指定发送报告的频率。在"收件人"屏幕上，请点击 *"发送至所有全局管理员"*或 *"发送至所有域管理员"*来分别向您的全局或域管理员发送报告。如果您希望阻止某些管理员接收报告，请使用排除部分中的选项来指定您希望排除的人员。使用 *"额外收件人"*选项来指定您希望接收报告的任何其他电子邮件地址。

摘要

摘要部分的报告都是常规的小结报告，您可以使用它们以查看经处理的接收邮件数量较之外发邮件数量，合法邮件较之垃圾邮件的数量与类型，以及邮件占用的带宽量。

- **接收 vs. 外发邮件**——该报告显示了选中的 *域*在报告中指定的 *日期范围*内接收与外发的邮件总数。图表下的表格包含一些列分别用于接收与外发邮件，每一行与 *"摘要"*的时间周期对应，报告正是根据该时间周期绘制的（小时，天数与月数）。单击表格内的任一链接以打开邮件日志并显示与该条目对应的时间周期内经处理的接收与外发邮件。报告中的条目数受限于 *"最大记录"*设置。报告产生时，SecurityGateway 将从第一个 *摘要*时间周期开始绘制报告，直到其达到 *最大记录*值才停止。如果 *"最大记录"*这个值设置得不够高，报告可能无法完整地涵盖指定的 *"日期范围"*。要产生一份新报告，指定其参数并单击报告上方工具栏中的 *"查看"*。
- **合法 vs. 垃圾邮件**——该报告显示了选中的 *域*在报告中指定的 *日期范围*内合法邮件较之垃圾邮件的总数。垃圾邮件就是那些被识别为垃圾邮件、诈骗，包含病毒一类的邮件。图表下的表格包含一些列分别用于合法与垃圾邮件，每一行

与 *"摘要"*的时间周期对应，报告正是根据该时间周期绘制的（小时，天数与月数）。单击表格内的任一链接以打开邮件日志并显示与该条目对应的时间周期内经处理的合法与垃圾邮件。报告中的条目数受限于 *"最大记录"*设置。报告产生时，SecurityGateway 将从第一个*摘要*时间周期开始绘制报告，直到其达到*最大记录*值才停止。如果 *"最大记录"*这个值设置得不够高，报告可能无法完整地涵盖指定的 *"日期范围"*。要产生一份新报告，指定其参数并单击报告上方工具栏中的 *"查看"*。

- **垃圾邮件分析**——该报告显示了选中的*域*在报告中指定的*日期范围*内所有垃圾邮件的总数，并根据类型加以分类。垃圾邮件被分为六类：垃圾邮件[125]，病毒[146]，诈骗[148]，滥用[172]，不完整与用户。*不完整*分类用于所有的超时会话，客户端关闭套接字、或在发送数据前启用退出命令的会话。SMTP 在该分类下无法进行探测。*用户*类别用于 阻止列表[205]、内容过滤器规则[195]、附件过滤[203]和自定义 Sieve 脚本[219]。剩下的分类与其对应的安全[124]部分有关。图表下的表格包含一些列分别用于每一种类型，每一行与*摘要*的时间周期对应，报告正是根据该时间周期绘制的（小时，天数与月数）。单击表格内的任一链接以打开邮件日志并显示与该◆◆目对应的时间周期内经处理的那一类垃圾邮件。报告中的条目数受限于 *"最大记录"*设置。报告产生时，SecurityGateway 将从第一个*摘要*时间周期开始绘制报告，直到其达到*最大记录*值才停止。如果 *"最大记录"*这个值设置得不够高，报告可能无法完整地涵盖指定的 *"日期范围"*。要产生一份新报告，指定其参数并单击报告上方工具栏中的 *"查看"*。
- **垃圾邮件 - 国家排行**—此报告按国家显示指定*域*和*日期范围*内收到的垃圾邮件数量。
- **邮件占用的总带宽**——该报告显示了在其中指定的*日期范围*内邮件占用的带宽总量。图表下的表格包含一些列用于占用的带宽总量，每一行与*摘要*的时间周期对应，报告正是根据该时间周期绘制的（小时，天数与月数）。单击表格内的任一时间周期以打开邮件日志并显示在那段时间经处理的邮件。报告中的条目数受限于 *"最大记录"*设置。报告产生时，SecurityGateway 将从第一个*摘要*时间周期开始绘制报告，直到其达到*最大记录*值才停止。如果 *"最大记录"*这个值设置得不够高，报告可能无法完整地涵盖指定的 "日期范围"。像这部分中的所有报告一样，要产生一份新报表，指定其参数并单击报告上方工具栏中的*查看*。

接收邮件

接收邮件部分中的报告只处理接收的邮件。您可以产生报告，详述所有经处理的接收邮件，报告根据邮件数量列居首位的邮件收件人，以及根据累积的邮件大小排行第一的收件人。

- **经处理的接收邮件**——该报告显示了选中的*域*在其中指定的*日期范围*内经处理的接收邮件的总数。图表下的表格包含一列，显示了在每个 *"摘要"*时间周期内经处理的接收邮件的总数，报告正是根据该时间周期绘制的（小时，天数与月数）。单击表格内的任一时间周期链接以打开邮件日志，来显示在该段时间内经处理的接收邮件。报告中的条目数受限于 *"最大记录"*设置。报告产生时，SecurityGateway 将从第一个*摘要*时间周期开始绘制报告，直到其达到*最大记录*值才停止。如果 *"最大记录"*这个值设置得不够高，报告可能无法完整地涵盖指定的 *"日期范围"*。要产生一份新报告，指定其参数并单击报告上方工具栏中的 *"查看"*。
- **国家排行**—此报告显示在指定的*域*和*日期范围* 期间，入站邮件来自的国家排行。

- **顶级邮件收件人**——该报告显示了选中的*域*在其中指定的*日期范围*内接收邮件最多的收件人。图表下的表格有一列用于收件人，还有一列用于每个收件人收到的邮件数量。单击任一收件人以打开邮件日志，以显示在报告中的日期范围内收件人所收到的邮件。要产生一份新报告，指定其参数并单击报告上方工具栏中的*"查看"*。
- **根据累积邮件大小的顶级收件人**——该报告显示了选中的*域*在其中指定的*日期范围*内根据累计的接收邮件的邮件大小或占用带宽列居首位的收件人。图表下的表格有一列用于收件人，还有一列用于每位收件人收到的邮件大小总和。单击任一收件人以打开邮件日志，以显示在报告中的日期范围内收件人所收到的邮件。要产生一份新报告，指定其参数并单击报告上方工具栏中的*"查看"*。

出站邮件

"出站邮件"部分中的报告只处理出站邮件。您可以生成报告，详述所有经处理的出站邮件，报告根据邮件数量列居首位的邮件发件人，以及根据积累的邮件大小排行第一的发件人。

- **经处理的外发邮件**——该报告显示了选中的*域*在其中指定的*日期范围*内经处理的外发邮件的总数。图表下的表格包含一列，显示了在每个*"摘要"*时间周期内经处理的外发邮件的总数，报告正是根据该时间周期绘制的（小时，天数与月数）。单击表格内的任一时间周期链接以打开邮件日志，以显示在该段时间内经处理的外发邮件。报告中的条目数受限于*"最大记录"*设置。报告产生时，SecurityGateway 将从第一个*摘要*时间周期开始绘制报告，直到其达到*最大记录*值才停止。如果*"最大记录"*这个值设置得不够高，报告可能无法完整地涵盖指定的*"日期范围"*。要产生一份新报告，指定其参数并单击报告上方工具栏中的*"查看"*。
- **顶级邮件发件人**——该报告显示了自选中的*域*在其中指定的*日期范围*内外发邮件最多的发件人。图表下的表格有一列用于发件人地址，还有一列用于出站邮件的数量。单击任一发件人地址以打开邮件日志，以显示在报告中的日期范围内该用户发送的外发邮件。要产生一份新报告，指定其参数并单击报告上方工具栏中的*"查看"*。
- **根据累积邮件大小的顶级发件人**——该报告显示了自选中的*域*在其中指定的*日期范围*内根据累计外发邮件的邮件大小或占用带宽列居首位的发件人。图表下的表格有一列用于发件人地址，还有一列用于每位用户发送的邮件大小总和。单击任一发件人地址以打开邮件日志，以显示在报告中的日期范围内该用户发送的外发邮件。要产生一份新报告，指定其参数并单击报告上方工具栏中的*"查看"*。

反垃圾邮件

"反垃圾邮件"部分中的报告允许您快速得知当前哪个域会向您用户发送最多的垃圾邮件，您的哪个用户收到最多的垃圾邮件。

- **顶级垃圾邮件域**——该报告显示了向选中的*域*在其中指定的*日期范围*内发送垃圾邮件最多的域。图表下的表格有一列用于发送垃圾邮件的域，还有一列用于收到的发自该域的邮件数量。单击列表中的任一域以打开邮件，以显示在报告中的日期范围内自该域发至您用户的邮件。要产生一份新报告，指定其参数并单击报告上方工具栏中的*"查看"*。

- **顶级垃圾邮件收件人**——该报告显示了选中的*域*在其中指定的*日期范围*内接收垃圾邮件最多的收件人。图表下的表格有一列用于收件人地址，还有一列用于收到的垃圾邮件数量。单击任一收件人地址以打开邮件日志，以显示在报告中的日期范围内该用户收到的垃圾邮件。要产生一份新报告，指定其参数并单击报告上方工具栏中的*"查看"*。

- **国家排行**—此报告显示在指定的*域*和*日期范围*期间，您收到的垃圾邮件所来自的国家排行。

反病毒

反病毒部分中的报告允许您快速地得知被 SecurityGateway 阻止的接收与外发邮件中的病毒数与精确的病毒种类。

- **被阻止的入站病毒**——该报告显示了选中的*域*在其中指定的*日期范围*内被 SecurityGateway 阻止的包含病毒的接收邮件总数。图表下的表格包含一列，显示了在每个*摘要*时间周期内被阻止的携带病毒的接收邮件总数，报告正是根据该时间周期绘制的（小时，天数与月数）。单击表格内的任一时间周期链接以打开邮件日志，以显示在该段时间内被阻止的携带病毒的接收邮件。报告中的条目数受限于*"最大记录"*设置。报告产生时，SecurityGateway 将从第一个*摘要*时间周期开始绘制报告，直到其达到*最大记录*值才停止。如果*"最大记录"*这个值设置得不够高，报告可能无法完整地涵盖指定的*"日期范围"*。要产生一份新报告，指定其参数并单击报告上方工具栏中的*"查看"*。

- **根据名称的顶级入站病毒**——该报告显◆◆◆了选中的*域*在其中指定的*日期范围*内被 SecurityGateway 阻止的在接收邮件中出现最多的病毒。图表下的表格有一列列出了被阻止的病毒名称，还有一列列出了每个病毒的事例数。单击任一病毒名称以打开邮件日志，以显示在报告中的日期范围内包含被阻止的特定病毒的接收邮件。要产生一份新报告，指定其参数并单击报告上方工具栏中的*"查看"*。

- **被阻止的出站病毒**——该报告显示了自选中的*域*在其中指定的*日期范围*内被 SecurityGateway 阻止的包含病毒的外发邮件总数。图表下的表格包含一列，显示了在每个*摘要*时间周期内被阻止的携带病毒的外发邮件总数，报告正是根据该时间周期绘制的（小时，天数与月数）。单击表格内的任一时间周期链接以打开邮件日志，以显示在该段时间内被阻止的携带病毒的外发邮件。报告中的条目数受限于*"最大记录"*设置。报告产生时，SecurityGateway 将从第一个*摘要*时间周期开始绘制报告，直到其达到*最大记录*值才停止。如果*"最大记录"*这个值设置得不够高，报告可能无法完整地涵盖指定的*"日期范围"*。要产生一份新报告，指定其参数并单击报告上方工具栏中的*"查看"*。

- **根据名称的顶级出站病毒**——该报告显示了自选中的*域*在其中指定的*日期范围*内被 SecurityGateway 阻止的在外发邮件中出现最多的病毒。图表下的表格有一列列出了被阻止的病毒名称，还有一列列出了每个病毒的事例数。单击任一病毒名称以打开邮件日志，以显示在报告中的日期范围内包含被阻止的特定病毒的外发邮件。要生成一份新报告，指定其参数并点击报告上方工具栏中的"查看"。

性能监控计数器

除了此处列出的报告选项外，SecurityGateway 还提供各种性能计数器，供 Windows 性能监控器使用，使您可以实时监控 SecurityGateway 的状态。提供许多计数器，例如活动的入站和出站 SMTP 会话数、排队等待投递的邮件数、隔离的邮件数、SecurityGateway 已运

行多长时间、域和用户计数等。**请注意：**以下计数器仅每分钟更新一次：投递队列、管理隔离、用户计数、域计数。

要在 Windows 中使用计数器：

1. 打开 "控制面板"中的 "管理工具"，然后双击 "性能监控器"（或运行 **perfmon**）。
2. 3. 在 "监控工具"下请点击 "性能监控器"，然后点击工具栏上的 "+"（添加）来打开 "添加计数器"对话框。
3. 在 "可用的计数器"下方的列表中，点击 **SecurityGateway**，然后点击 "添加 >>"来添加所有 SecurityGateway 计数器。或者，如果您不想添加所有计数器，请展开 SecurityGateway 组并选择任何所需的计数器，然后点击 "添加 >>"。
4. 点击 "确定"。

请注意：要从在另一台机器上运行的 SecurityGateway 上查看性能计数器，您必须启用 "远程注册表"服务，并能通过任何防火墙进行访问。

索引

- 2 -

- A -

- C -

- D -

- E -

- F -

- H -

- I -

- L -

- M -

- P -

- Q -

- R -

- S -

- T -

– U –

– V –

– W –

– Z –