MDaemon Technologies 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，为您的网络架构提供全面的保护，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, 反病毒, 反诈骗, 以及反滥用技术以达到 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与 SIEVE 脚本编辑器，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：

控制面板


您登录 SecurityGateway for Email Servers 的第一个页面是“仪表盘”。 控制面板的

登陆页面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。

控制面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，提供链接以管理您的注册与激活，并列出了当前存在的域与用户数。 它还提供了通往域列表的链接以管理您的域和用户。 存在可用的软件更新时，此部分还将提供有关更新详细信息的链接。

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，邮件占用的总带宽，合法 vs. 垃圾邮件，垃圾邮件分析，顶级邮件收件人，与顶级垃圾邮件域。 每个报表都显示了近 24 小时内的统计数据。

左边窗格的控制面板菜单中有一条通往控制面板登陆页面的链接，还有链接通往您的我的帐户选项，该选项允许您管理您自己的帐户设置，隔离区与邮件日志。

域管理员将只能看到他们具有管理权限的域的统计信息和选项。

设置/用户

*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帐户，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：

- **帐户**——帐户部分位于*设置/用户*菜单之下，包含了关于您的 SecurityGateway 用户帐户与域的选项。 该部分之下有五个与帐户相关的链接，它们包括一些选项用于创建域与用户帐户，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**——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。 比如，您将使用这部分的选项来指定您用户的邮件帐户所位于的服务器，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)**—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**——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**——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**——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

*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**——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。 有八个反垃圾邮件功能列于该部分之下，包括一些选项用于通过使用启发式与贝叶斯分析，DNS 与 URI 黑名单，灰名单等来识别与防范垃圾邮件。

•**反病毒**——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。 为了提供一个广泛层次的病毒保护，SecurityGateway 提供两款反病毒引擎： Clam AntiVirus (ClamAV™) 和 CYREN Anti-Virus。 ClamAV 是一套开源的(GPL) 反病毒工具集，特别为邮件网关而设计。 CYREN AV 提供可靠的保护以防（潜在的）恶意程序。 它整合了传统的反病毒方法和最新的前瞻性技术。 SecurityGateway 还包含 CYREN 的爆发保护 ，为您提供了抵御病毒爆发的传统保护层。

•**反诈骗**——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，回叫验证等。

•**反滥用**——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： 邮件内容过滤与附件过滤。 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。 您可以全局性地也可以为每个域定义过滤限制。

•**黑名单**——黑名单是一些列表，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，但是在黑名单的操作页面，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，并且黑名单本身也可进行全局或特定域的设置。

•**白名单**——白名单是一些列表，如果您希望让某些邮件免于一系列安全限制，会于此列出其邮件地址，主机与 IP 地址。 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白名单上时，将它们从中排除。 每个白名单都可以进行全局或特定域的设置。

•**Sieve 脚本**—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。

邮件/队列

邮件/队列菜单为您提供两部分的设置：

•**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，如发件人被列入黑名单，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。 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*。 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

日志菜单帮助您访问以下三部分：

•**邮件日志**——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**——您可以使用日志文件部分来查看 SecurityGateway 贮存在您日志文件夹中的各种日志文件。 不像邮件日志，日志文件并不贮存在数据库中，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，比如系统日志，接收与外发日志，病毒库更新日志等等。

•**配置**——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

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，位于 www.altn.com.cn。

获得帮助

请访问 www.mdaemon.com/Support/ 以获得 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、社群论坛等。

中文联系方式
电子邮件：service@yuncan.com

联系电话：021-50583875