Mate-Email-UTM

全方位邮件安全解决方案

目录

项目目标

建置 Mate 邮件安全解决方案，协助企业组织免于垃圾邮件与病毒邮件的威胁，确保企业组织邮件安全。

概述

垃圾邮件发送者除了以赚钱为目的外，其很重要的一点就是要逃脱邮件安全解决方案的过滤，道高一尺魔高一丈，邮件过滤与反过滤之间的斗争已经持续了十几年。

第一代垃圾邮件大部分是 ASCII 纯文字内容并带有一定的随机性，容易使用关键词过滤掉此种邮件。但同时，垃圾邮件也在不断的演化，最新的垃圾邮件已经包含了相当复杂的技术包括重度的随机化，隐藏发送端，以及使用 HTML 语法的反过滤技术等。垃圾邮件发送者永远都在想方设法逃避过滤以便从垃圾邮件中获取好处。

随着信息时代到来，电子邮件在人们的生活中扮演越来越重要的角色，企业进行业务往来更加依赖于邮件系统的正常运作。邮件系统的安全以及信息传递内容的管理也变得极为重要。然而，企业资源不断地遭到病毒程序、垃圾邮件、非法内容的侵犯，干扰企业正常运作，造成邮件系统的瘫痪，泄漏企业机密信息，损害企业的信誉甚至导致企业陷入法律纠纷。

也因此邮件安全解决方案的建置，对客户而言是刻不容缓的议题。

邮件安全问题的现状

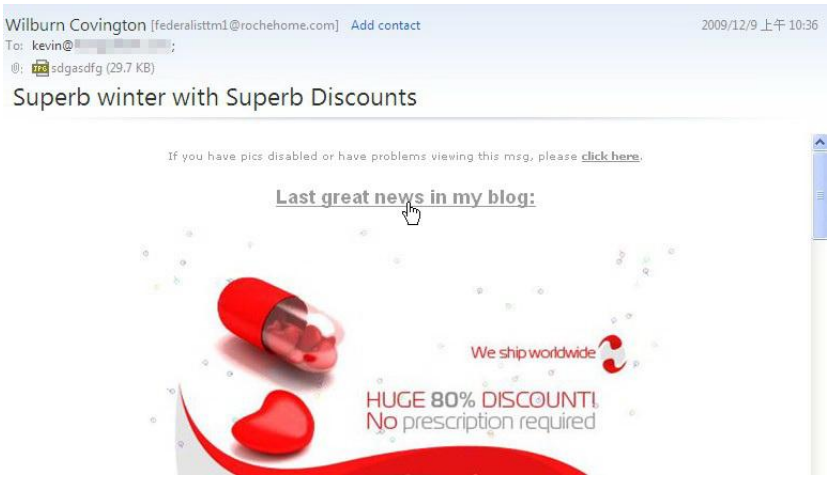
- **垃圾邮件的定义**

垃圾电子邮件是指用户未主动请求或同意接收的电子刊物、电子广告和各种形式的电子宣传品等电子邮件，没有明确发信人、发信地址、退信方式、发信人和收信人之间没有任何可识别关系的电子邮件，含有伪造信息源、发信地址、路由信息或收信人不存在的电子邮件。

- **垃圾邮件的类型**

从电子邮件诞生的那天起，伴随着电子邮件的威胁就从来没有中断过，从最早的电子邮件病毒到目前流行的基于电子邮件的“网络钓鱼”（Phishing），电子邮件的威胁方式越来越多，危害也越来越大。

而伴随着电子邮件系统出现的垃圾邮件问题已经持续了十几年，从最初的纯文件格式的垃圾邮件开始，已经经历了相当大的变化，从早期的文字型垃圾邮件、图片型垃圾邮件之外，现今还包括常见的钓鱼型垃圾邮件与夹带恶意程序压缩文件之垃圾邮件，目的就是透过吸引人的标题与内容，来进行收件者个人信息的窃取与植入木马程序等意图。



图、钓鱼型垃圾邮件

- **垃圾邮件发送者所采用的手段**

从商业杂志的调查结果来看，如果垃圾邮件接收者的回复率有 0.05%,也就是 2000 个人里只要有一个人对这些邮件做回复，一些垃圾邮件发送者一个月就可以获取百万的收益。如此高的回报率使得发送者们想方设法来逃避反垃圾邮件的过滤。其往往采用如下的规避手段：

- **HTML 的邮件内容变化：**利用 HTML 来改变邮件内容是垃圾邮件目前最新最有力的反过滤手段，根据 2003 年 6 月的调查结果，超过 80%的成人内容垃圾邮件采取的是这种手段。对垃圾邮件来说，用这种方法可以：
  - **吸引注意：**可通过 Flash 或语音等手段来迅速抓住接收者的注意力
  - **方便跟踪：**往往一旦图片被下载，其内置的追踪连结可以使得垃圾邮件发送者确认目前邮件地址是否有效
  - **方便邮件内容随机化和混乱化：**很容易利用 HTML 标签和 HTML table 等手段来随机化邮件内容。由于采用 HTML 后可对邮件做无数的随机和混乱化，垃圾邮件发送者大量的采用这种方式来逃避邮件过滤。

- **URL 的伪造：**垃圾邮件经常带有看上去正常的邮件内文和合法的 URL 连结，而实际上当用户相信这是一个合法连结采取点击等后续动作时，却被连结到有问题的网址。

- **通过 Open Proxy 来隐藏身份：**垃圾邮件经常会通过 Open Proxy（是错误配置或者被病毒所感染的机器，允许所有的网络服务流量通过它来中继转发）来隐藏真实的 IP 地址等身份要素。Open Proxy 并不同于常见的开放邮件中继（open smtp relay）。邮件中继有时在某些情况下需要使用，而且其隐藏发送源的能力也比较弱，绝大多数 MTA（邮件传输代理）都会在中继邮件前加上 Received 域，使得原始的发送端包含在该字段里。而 Open Proxy 允许几乎所有的机器共享它的因特网连接，完全转换为 Proxy 本身的地址来通过 HTTP POST 方式来向外部邮件服务器的 25 埠传送邮件内容，这使得接收者不可能发现真正的原始发送源，因此大多数垃圾邮件都是通过 Open Proxy 的方式来发送的。

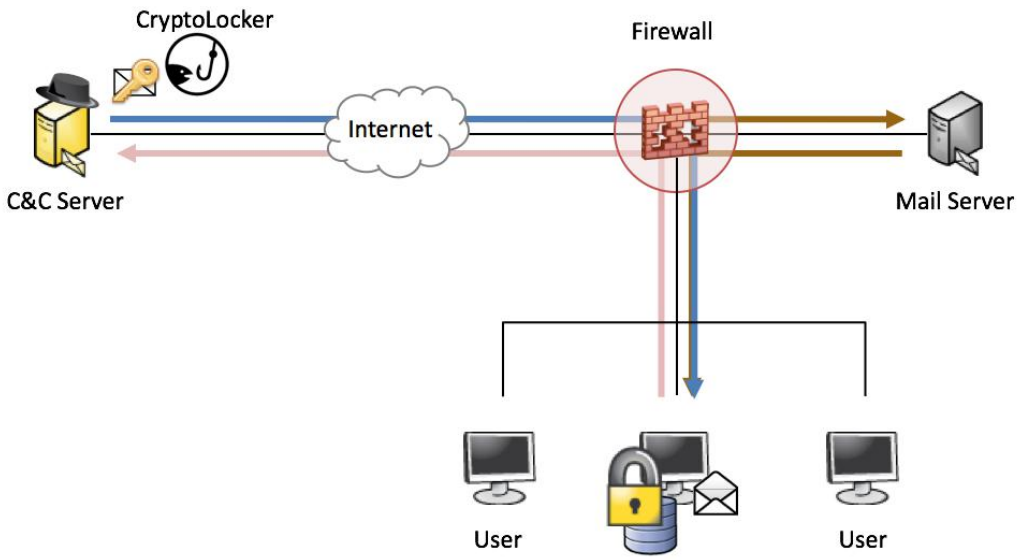
- **暴力攻击盗用弱口令邮箱帐号传播垃圾邮件：** 攻击者通过扫描互联网上所有开放了 25 端口且支持 SMTP 和 POP3 身份认证的邮件服务器进行大量的弱口令密码字典暴力登录探测，以持续不断尝试登录的攻击方式猜测破解用户的邮箱密码；一但弱密码被探测破解出来，则会利用该用户帐号的身份大量转发垃圾邮件，伪装垃圾邮件发送者身份，浪费公司的网络带宽和服务器资源，导致邮件系统队列大量堆积堵塞，甚至导致公司邮件出口 IP 和域名信誉降低被列入黑名单导致邮件无法发送；

- **新型恶意邮件攻击威胁**

  从 2012 年～2017 年大量爆发的携带勒索病毒，银行木马等恶意软件的攻击

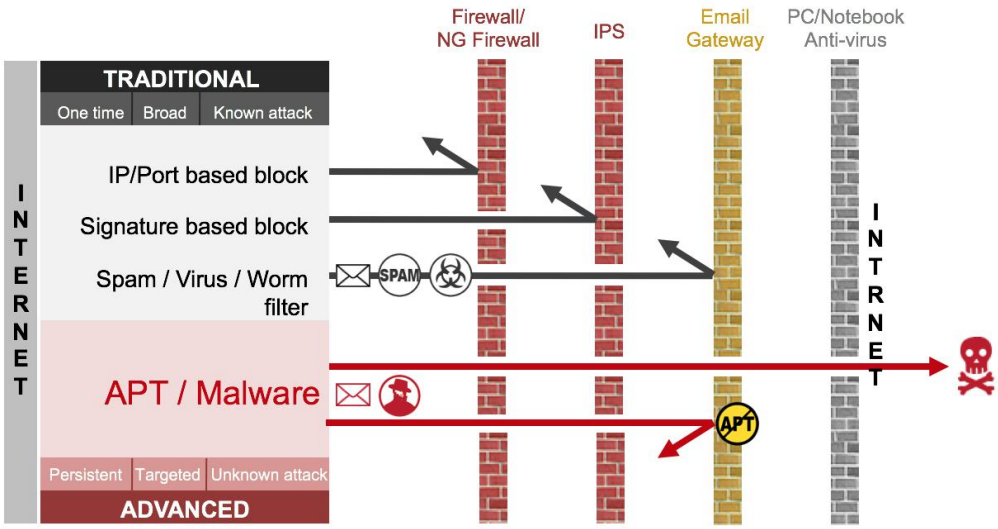
邮件趋势越来越多，而且病毒变种日新月异，这些会对企业信息安全，数据安全造成巨大安全风险和恶意程序；企业电子邮件也成为了这些恶意软件的重要攻击和传输途径；深层次，持续性，有针对性的目标 APT 攻击已经突破了常规的邮件安全防御手段，全新构造设计的邮件内容，全新变种的恶意程序，且通过正规邮件渠道针对性的仅发送特定目标邮箱；这种 APT 邮件已经无法被常规的垃圾邮件引擎和居于病毒特征库识别的常规放病毒引擎所识别；因为根本就没有已知的威胁特征可以进行比对和识别；

以下是一封勒索邮件进行数据加密勒索攻击的完整流程



1， 攻击者精心构造了一封钓鱼邮件给用户，穿透常规网络安全设备，甚至常规的邮件防火墙和放病毒软件；
2， 用户点击恶意链接或者运行了附件文件则会主动连接黑客的 C&C 服务器下载并运行 CryptoLocker 恶意加密勒索程序加密用户电脑上的数据。
3， 显示了锁信息，并要求用户及时支付赎金用于数据解密；

因此我们知道新型的 APT 攻击是可以完全规避所有居于静态特征码对比的安全产品检测的



因此传统的防垃圾邮件手段，和静态的病毒防御机制已经远远不能胜任当前企业所可能面临信息安全风险，必须采用全新的机制和技术手段来应对这些新型的 APT 渗透式威胁；

Mate 邮件安全解决方案目标

电子邮件是现代文明社会中最重要的传播媒介之一，许多的研究中也表明，电子邮件是除了传统的电话与传真之外最重要的沟通工具。根据估计，对企业组织而言，电子邮件的发送和接收数量正在以每年 20％左右的成长速度向上成长，同时公司组织传输的电子邮件中，更有超过 60%以上的比率均包含重要的公司组织数据，这些事实都证明了电子邮件的重要性不仅可以协助企业组织与员工间的沟通，更可以协助拓展业务与协助公司成长。

- **避免重要邮件被垃圾信淹没**

电子邮件通常被视为一个沟通工具，但是经由电子邮件所传输的讯息与数据，其重要性与一般纸本档毫无差异，例如业务部门会透过电子邮件传输产品价格数据给客户；行政部门也会透过电子邮件传达重要公司政策与规定；而财务部门更透过电子邮件传输重要的财务相关数据给股东会成员等。简单来说，电子邮件上所传输的信息已经不单纯是一般的讯息传递，而是公司组织的重要数字资产，若是由于垃圾邮件数量过多造成收件者错误的判断，而忽略重要的信件，将会严重影响企业组织日常营运，因此必须透过邮件安全机制来过滤垃圾邮件，以确保企业组织日常营运不受影响。

- **避免邮件病毒攻击**

多数的垃圾邮件经常包含为数不少的病毒邮件或者钓鱼信件，而这类型邮件会透过吸引的标题或者附件档案，对个人或者企业组织进行重要数据的窃取或者对收件者的计算机植入木马程序以便从远程控制，进行更多的攻击行为。对个人而言有可能造成个人资料外泄、财产损失；对企业组织而言，则有可能造成重要机密外泄、客户名单外流，进而造成财产损失与企业名誉伤害。

- **减少企业组织频宽的浪费**

根据研究报导，垃圾邮件约占全部邮件的 70%~90%之间，企业营运的网络频宽若是都用来处理这些垃圾邮件，势必对正常企业组织每日营运所需的网络频宽造成排挤效应，所造成的影响不仅让内部员工无法正确的进行网络联机，甚至可能让客户无法连至企业组织重要网站，而造成财产的损失。因此垃圾邮件的防御机制必须能够有效的阻挡外来的垃圾邮件，以避免企业组织营运受到影响。

- **避免邮件主机遭受攻击**

传统的邮件主机建置方式，由于需要接收外来的邮件，因此多数是将邮件主机置放于企业外部网络区段，这类型建置在现今的网络环境是相当危险的，因为等于

提供了黑客能够直接做网络沟通的机会，一旦能够做网络沟通，就有可能遭受到攻击，而导入邮件安全机制后，企业组织可以将邮件主机置放于企业内部网络区段，只将邮件安全设备置放于外部来接收与扫描邮件，如此一来，黑客将无法直接与邮件主机沟通，自然也大大的降低邮件主机被攻击的机会。

- **全面防御新型 APT，钓鱼等邮件威胁**

通过先进的云端沙箱模拟执行，突破传统的静态特征对比的模式和手段；采用主动引爆未知恶意文件，通过动态分析程序运行行为特点的方式，动态主动深层的分析是否包含恶意和危险行为,从而判定是否是具有恶意行为的新型渗透式 APT 程序；可以在常规反垃圾邮件以及防病毒邮件手段之后，对其进行更加全面的检测和安全防护；保护企业的邮件安全，确保任何变种的木马与钓鱼和鱼叉式攻击邮件进入企业的办公环境；

Mate 邮件安全解决方案

- **Mate Email UTM 设备概述**

Mate Email UTM 是 Mate 公司为企业提供易于部署的基于网关的综合电子邮件安全解决方案,可以保护您的组织不受基于电子邮件的恶意垃圾邮件或病毒的攻击，同时确保仍然可以通过电子邮件进行有效通信。通过联机控管、SMTP 交谈检查、反垃圾邮件、防病毒和邮件策略以及邮件归档功能整合到一台设备中来提供整合性的的电子邮件解决方案，Mate Email UTM 系列设备实现了当前可用的最有效、最准确和易于部署的电子邮件安全解决方案。

电子邮件威胁的领域正在不断扩张。如果不对邮件服务器的 SMTP 联机进行有效的控制，恶意发件端来的威胁就会损害电子邮件的安全。在许多邮件系统中，几乎所有发件端都可以连接到邮件服务器。 在另一些邮件系统中，由于过分限制对电子邮件服务器的 SMTP 联机而妨碍了一些重要的业务功能。 Mate Email UTM 系列设备中的电子邮件防火墙和搭配 CGAC 全球监控机制确保合法发件人可以正常使用 SMTP 联机服务，并且使滥用邮件的发件人很难或根本无法连接到邮件服务器而无法消耗邮件服务器资源。

除了根据发件人 IP 以及邮件内容来进行阻挡威胁外，防止恶意内容也是非常必要的。 虽然现在制订了有关维护适宜工作环境的法律要求，但是在满足电子邮件策略标准方面，组织还是面临着越来越大的压力。Mate Email UTM 系列设备整合了三个方面的内容安全防护： 反垃圾邮件、防病毒和内容。 尽管这些经过公认的、行业领先的技术可以独立运行，但是当它们作为综合电子邮件安全解决方案的一部分运行时会更加有效。 例如，由于电子邮件防火墙可减少传入的电子邮件通信的数量，因此反垃圾邮件和防病毒过滤可以更有效地运行侦测邮件内容进行阻挡。

Mate Email UTM 电子邮件产品出色的拦截率使得拦阻垃圾邮件的有效性达 95% 以上，误报率不到百万分之一。 同类技术只能捕获不到 90% 的垃圾邮件或病毒，也就是说它们的误报率较高，不能让用户和管理员相信它们可以实现整合的电子邮件策略管理。Mate Email UTM 系列设备允许您创建任意过滤策略，满足您的特定要求。

Mate Email UTM 一直在不断创造新的过滤技术。每一种技术都经过严格的检验以保证不会对 Mate 近乎苛刻的垃圾邮件过滤准确性造成影响，Mate Email UTM0 系列设备目前的准确率可以达到 99.9999%，也就是说检查 100 万封邮件，

才会错误的将 1 封合法邮件误判为垃圾邮件。

同时，Mate Email UTM 系列的自动化过滤器更新和整合式的设备形式避免了几乎所有一直存在的管理负担。Mate Email UTM 系列设备的主要特点是它的 Web 的管理控制台，可以提供充分的控制、灵活性和可视性。使用能够识别 LDAP 的电子邮件策略、丰富的邮件处理选项、可通过 Web 访问的隔离区以及过滤自定义工具，管理员可以对组织内不同的群组或用户实施公司或部门针对垃圾邮件和不适当邮件制定的策略。 为了进一步洞察攻击趋势和攻击统计信息，还提供了多种报告，它们具有非常灵活的调度和发送选项。

Mate Email UTM 系列设备整合了多种高效且有差异的电子邮件威胁防护，同时可降低电子邮件通信的入站流量。 这些特征如果与设备固有的易管理和易部署优点相结合，可以帮助减少电子邮件安全的总拥有成本。节省的这些成本可以通过减少的硬件、网络频宽和管理员资源成本体现出来。由于这种功能强大的组合受到 Mate 的支持，因此客户还可以从行业领先的安全提供商所提供的支持和服务中受益。

Mate Email UTM 的使用方式

Mate Email UTM 系列设备的用途非常灵活，根据您的网络规模和电子邮件处理的需要，它们可以执行多种不同的功能。每台 Mate Email UTM 系列设备都可部署为：

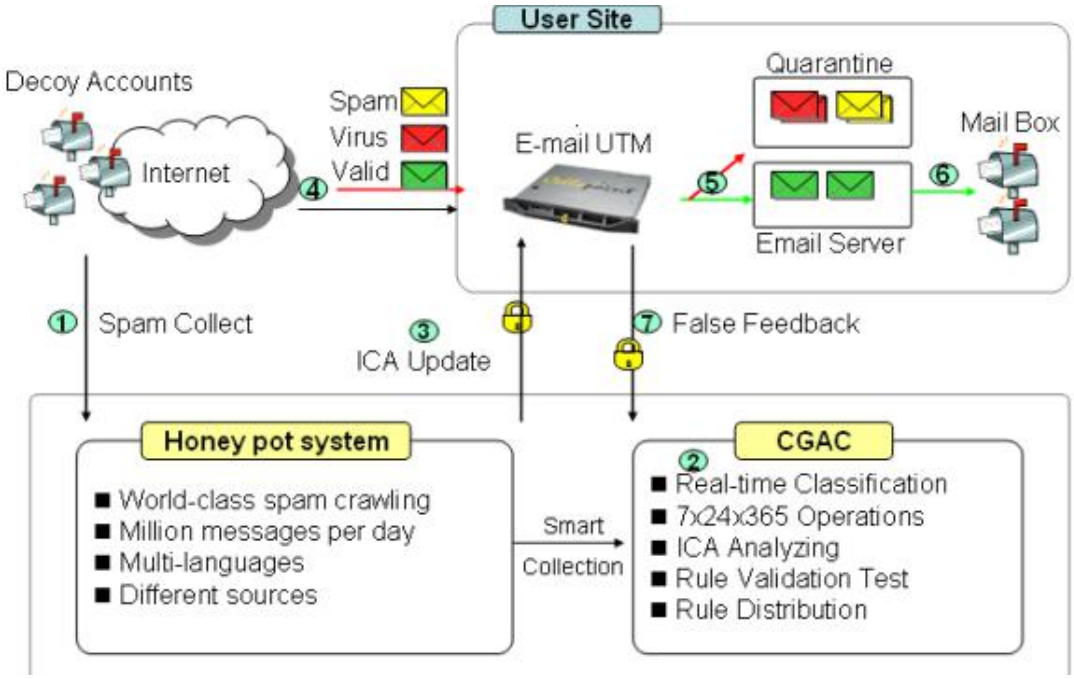
- Mail Gateway：如果只部署为 Mail Gateway，Mate Email UTM 系列设备将会过滤电子邮件。在一个完整的 Mate 反垃圾邮件系统中，可以有一个或多个 Mate Email UTM 布署成为 Mail Gateways，进行垃圾邮件扫描，并且搭配其中一台 Mate Email UTM 布署成为 Mail Reporter 用以保存邮件数据以及做为邮件隔离区。Mate Email UTM 系列设备可以与现有电子邮件或 Groupware 服务器一起工作。
- Mail Reporter：每个 Mate Email UTM 系列安装都有一个 Mail Reporter，在一个完整 Mate Email UTM 服务架构中，至少会配置一台 Mate Email UTM 成为 Mail Reporter。Mail Reporter 主要负责邮件储存、邮件隔离产生报表和用户管理等功能。终端用户可以登入 Mail Reporter 来查看隔离区中的垃圾邮件，还可以设置他们黑白名单。客户可以再指定另外一台 Mate Email UTM 做为 Redundant Mail Reporter，用以当做 Mail Reporter 的备援。
- Mail Gateway 与 Mail Reporter：执行上述两种功能。适用于小型安装。

在 1000 人以下的客户中，我们可以配置一台 Mate Email UTM，同时执行 Mail Gateway 以及 Mail Reporter 的工作。此台 Mate Email UTM 同时进行邮件扫描，并且让用户登入管理他们的邮件。

Mate GAC 工作原理

Mate Email UTM 主要是透过 Mate Global Antispam Center 发布的垃圾邮件规则来针对垃圾邮件进行阻挡。以防毒软件为例，厂商在全世界收及病毒的样本，然后传送到病毒监控中心，找出特征及解毒后，发布更新到全世界的使用者计算机中。

Mate 新一代的防垃圾邮件解决方案也采用此一概念，在全世界设置垃圾邮件诱捕信箱，搜集全世界垃圾邮件样本，经过计算机与人工筛选后，找出规则，再及时更新到 Mate 全球的防垃圾邮件网关，由于信件数量每日达到上百万封，样本数丰富，误判率低，可以非常有效的阻挡垃圾邮件攻击。以下是 Mate Global Antispam Center 介绍：



1. Spam collect：主动搜集垃圾邮件样本是 Anti-spam 厂商分出高下的重要指标，Mate 在全球布署了数量庞大的诱补账号(Decoy Accounts)，组成一个世界级的搜集垃圾邮件样本的诱补系统(Honey pot system)，每天会搜集至少数百万封之全新样本或变种样本，包括 Internet 中不同语言及发送来源之取样。

2. CGAC：Mate 全球反垃圾邮件中心(Mate Global Anti-spam Center)是以

7*24*365 全时监控所诱补系统所搜集的样本，并实时做快速分类(Classification)，判断是否为突然暴大量之发送垃圾邮件殭尸网络攻击、图文件垃圾信(Image Spam)、PDF 或 ZIP 型变种垃圾邮件等，或是更改发送来源之原有之样本。在分析其特征及发送行为后，CGAC 值班的成员开始产生多种 ICA 的分析与可能的解药；再经由大量的样本做压力测试与误判测试，直到真正的 ICA 解药确定后，会予以编号及正式发布。

3. ICA Update：Mate 分布在全球各地之保固期内 Mate Email UTM 设备皆享有 CGAC 最新 Anti-spam 特征数据库更新，ICA Update 机制是以每小时更新最新的 ICA Rule，以实时防御变化多端的垃圾邮件困扰，此完全自动化机制可大符降低 MIS 人员维护负担。

4. 实际威胁发生：来自 Internet 的大量 Spam、Virus、Phishing Mail 及全新的攻击严重威胁 Mail Server，将 Mate Email UTM 布署在用户之网关(Gateway)端，可有效做好整体邮件威胁之防御与管理 UETM(Unified Email Threat Management)。

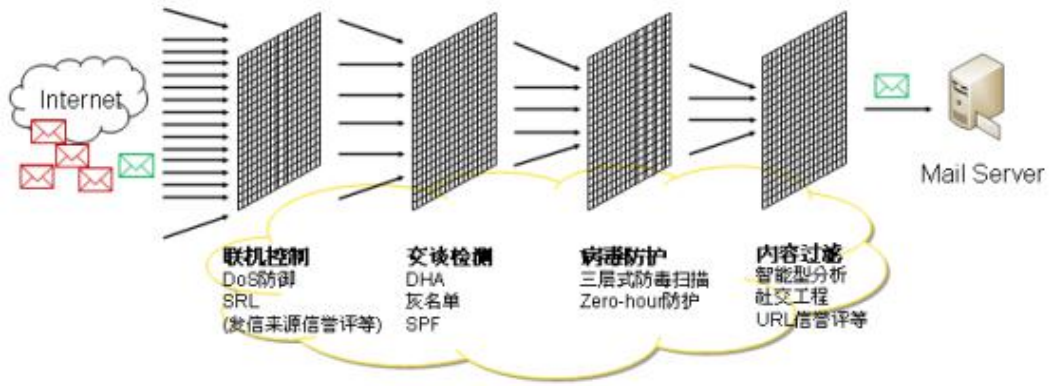
5. 与组织政策搭配：依客户端不同需求，信息主管(CIO)可规划与制定电子邮件安全规则，透过功能强大政策式(Policy-Based Engine)引擎设定全公司、部门及个人的政策，Mate Email UTM 依照政策以多层次过滤、拦截引擎将邮件分类及过滤。

6. 隔离与放行：Mate Email UTM 将正常的邮件后送至 Mail Server，其它有问题的 Spam、Virus、Phishing Mail 则暂存在隔离区(Quarantine Area)。

若万一发生误拦或漏拦情况，可透过直觉式回报接口将误判的邮件回报原厂，CGAC 同样地 7*24*365 监控回报情况，并且修正及更新 ICA 规则，使客户满意度维持业界 No.1。

CGAC 建立的垃圾邮件规则可以阻挡大部分的垃圾邮件。除了 CGAC 生成的垃圾邮件规则之外，Mate Email UTM 还有配备其它的垃圾邮件检测机制，可以使 Mate Email UTM 拦截率再提升。

Mate Email UTM 系列设备按如下方式处理邮件：



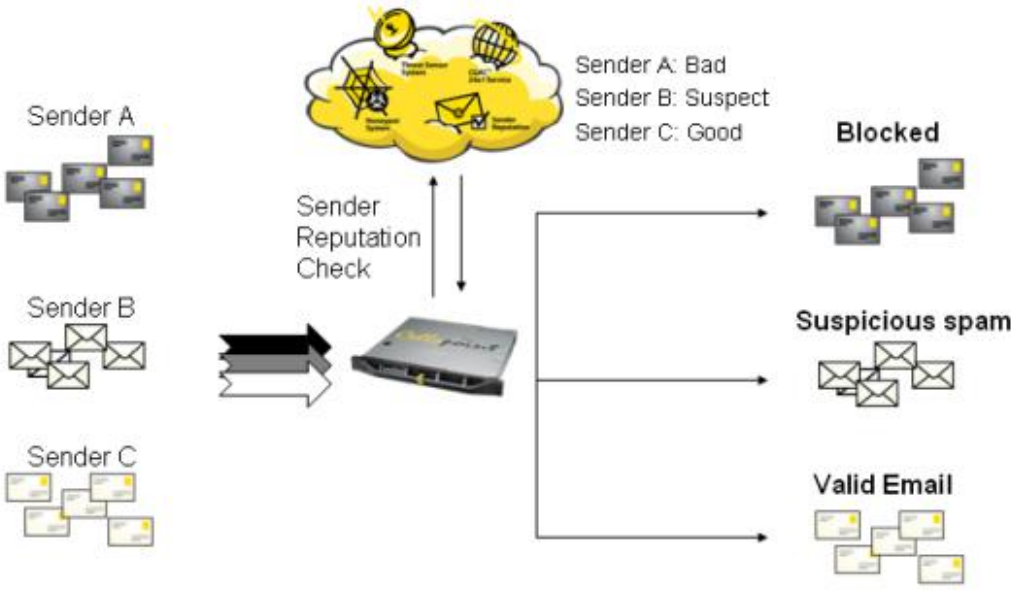
- 在网关中，Mate Email UTM 检查 SMTP 联机的 IP 地址，确定它是否来自已知的垃圾邮件寄件端或携带病毒的电子邮件寄件端。Mate Email UTM 会去查询 Mate Sender Reputation List，确定该联机 IP 的信誉，根据不同联机 IP 的信誉评等，可以进行不同的联机控管策略。
- 当 Mate Email UTM 接受 SMTP 联机后，会检查 SMTP 交谈是否合乎邮件中继政策(Relay)，若不合乎邮件中继政策，则拒绝接收该信件。
- 接收邮件进行病毒邮件扫描
- Mate Email UTM 防垃圾邮件过滤引擎确定每个收件人的过滤策略。
- 反垃圾邮件过滤器将邮件元素与 Mate 安全响应中心发布的最新过滤器进行比较，以确定邮件是否是垃圾邮件。
- 邮件政策内容过滤器检查邮件是否符合用户所设置的邮件政策。
- Mate Email UTM 根据过滤结果和邮件政策设置执行相应的操作。

Mate Email UTM 系列功能详细介绍

- **SMTP 联机控管**

  SMTP 联机控管机制是 Mate 第一个防护级别，它分析传入的 SMTP 联机并在邮件在过滤过程中得到进一步处理之前启用优先响应和操作。Mate Email UTM 可提供的联机控管机制如下：

  - **寄件人信誉判断防护：**CGAC 在 Internet 上搜集寄件人 IP 以及其发信频率、邮件质量并会对寄件 IP 进行信誉评等。Mate Email UTM 可以透过通过寄件人信誉来拒绝其联机或是限制其邮件发送频率，运作方式请参考下图。



- **SMTP 联机 Anti-DoS 防护：**Mate Email UTM 可提供相当精细的 Anti-DoS 防护功能。包含针对某段时间内若是该 IP 建立过多 SMTP 联机，Mate Email UTM 可以在指定时间内拒绝该 IP 对 Mate Email UTM 建立 SMTP 联机。
- **发信 Anti-DoS 防护：**若是该 IP 在侦测时间内发送过多信件，Mate Email UTM 可以在指定时间内拒绝该 IP 对 Mate Email UTM 建立 SMTP 联机。
- **账号发信频率防护：**若是有透过 Mate Email UTM 认证后发送信件，可以限定该账号的发信数目。这对于因为计算机中毒寄到外部的垃圾邮件防护特别有用。管理员不用担心因为使用者中毒发送大量邮件导致频宽用尽，或是造成公司发信被列在黑名单。
- **SMTP 联机行为安全控管：**若是该 IP 在侦测时间发送过多错误的 SMTP 指令，Mate Email UTM 可以在指定时间内拒绝该 IP 对 Mate Email UTM 建立 SMTP 联机。
- **SMTP 联机控管：**Mate Email UTM 针对总体 SMTP 联机数以及单一 IP 最大连数可以进行控管。若单一 IP 与 Mate Email UTM 建立过多 SMTP 联机，则有可能是 DoS(Denial of Service)等攻击行为，Mate Email UTM 可拒绝超过此上限之联机。
- **发信数量控管：**可针对单一 SMTP 联机进行发信总数量控管。
- **系统定义禁止的寄件人：**管理员可以定义哪些寄件 IP 不能对 Mate Email UTM 发送信件。

SMTP 协议检查

SMTP 联机协议检查机制是 Mate 第二个防护级别，它分析的 SMTP 联机并在邮件在过滤过程中得到进一步处理之前启用优先响应和操作。Mate Email UTM 可提供的联机控管机制如下：

- **寄件人伪冒检查：**Mate Email UTM 可以查询寄件端的 SPF 数据，来判别该寄件行为是否为伪冒的寄件行为并且进行阻档。
- **寄件人网域验证：**用以确认寄件网域是否存在。
- **账号搜集攻击(DHA)防护：**Mate Email UTM 可侦测到有搜集电子邮件地址的攻击尝试并且拒绝其联机。 账号搜集攻击是针对特定邮件网域上由字典产生的收件人地址的大量攻击活动。DHA 不仅会消耗目标电子邮件服务器上的资源，还会向垃圾邮件发件人提供有效电子邮件地址列表，并进一步发起垃圾邮件攻击。Mate Email UTM 可以搭配 LDAP 或是后端邮件主机进行收件人验证，并针对 DHA 攻击提供防护。
- **Greylist：**针对第一次的寄件行为，Mate Email UTM 会进行延迟接收。若是在指定时间内又在进行重寄，Mate Email UTM 会宇以接收进行内容过滤。Greylist 针对殭尸计算机发信行为的阻挡特别有用，因为殭尸计算机发送信件若是遇到错误，不会进行重寄。
- **DNS MX 记录检查：**这是一项对于垃圾邮件发送者采用虚假邮件地址的有效阻断技术。Mate Email UTM 在发自邮件地址的网域上进行查询。如果该域没有一个有效的 DNS MX 记录，这样发自地址就是无效的，该邮件就被分类为垃圾邮件。对回复邮件地址也可以进行相应查找。
- **Reverse DNS Lookup：**这是一种有效的垃圾邮件阻断技术，Mate Email UTM 对收到邮件的来源 IP 地址采用反向 DNS 查询，如果反向 DNS 查找提供的域与邮件上的来源 IP 地址相符合，该邮件被接受。如果不符合，则拒绝该邮件。
- **防制 BATV 退信攻击：**避免客户受到退信攻击。

防病毒技术

防病毒邮件扫描是 Mate Email UTM 第三防护级别。Mate Email UTM 整合 ClamAV、Sophos、Kaspersky 三家防毒引擎在 Mate Email UTM 内。三家防毒引擎可以同时运行进行扫描。防病毒功能和技术的范围包括以下各项：

- **自动更新：**Mate 会创建病毒特征和定义，并且一旦这些特征和定义可用，就立即在客户站点中进行更新。
- **病毒隔离通知信：**可将病毒性隔离，并依照需求寄送病毒通知信。

反垃圾邮件技术

垃圾邮件内容检查机制是 Mate 第三个防护级别。Mate Email UTM 系列设备并入了多层垃圾邮件扫描侦测机制，利用了业界领先的技术，并由分布在全球的操作中心提供支持。防垃圾邮件处理引擎利用多种不同的过滤技术，这些技术共同作用来最大限度地提高垃圾邮件检测的效率（有效性达 95% 以上），并最大限度地减少误报（每一百万个邮件中不到一个误报）。反垃圾邮件功能和技术的范围包括以下各项：

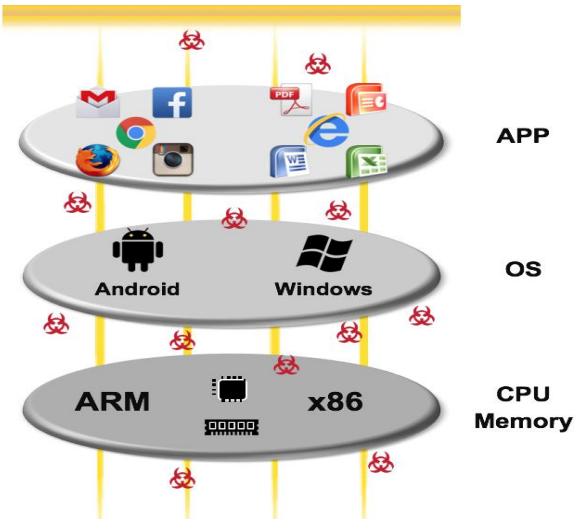
- **ICC/ICA：** Global Antipsam Center 收集世界上所有垃圾邮件样本并且产生垃圾邮件规则，Mate Email UTM 可定时更新这些规则以达到最佳的拦截率。
- **黑白名单：**设置公司的禁止的和允许的发件人列表（也称为黑名单和白名单）。来自允许的发件人的电子邮件通常会被发送（除非它包含病毒或蠕虫），来自禁止的发件人的电子邮件会可以根据您选择的方式进行处理。
- **关键词过滤：**提供基本的关键词过滤功能。Mate Email UTM 可以针对多种语言进行关键词过滤，并且还可以针对附文件中的关键词进行过滤。
- **更新的启发式过滤器：**根据垃圾邮件和合法邮件的已知特征来评估传入邮件的内容的过滤技术。Mate Email UTM 内建多种启发式评分规则，可以针对收到邮件进行评分，若是分数超过设定的门坎值，则会判定为垃圾邮件。
- **60 分钟更新：**每隔 60 分钟过滤器都会通过安全 HTTPS 从 CGAC 自动下载到客户站点。无需管理员干预。
- **垃圾邮件检测网络：**CGAC 在网络上布建数百万个 Honeypot，收集最新的垃圾邮件并将这些垃圾邮件内容与统计资料提交给 CGAC 进行分析。
- **回报漏拦的垃圾邮件：**终端最终用户可以登录到控制中心（一个基于 Web 的接口）将漏拦的垃圾邮件提交给 Mate。
- **全天候误报解决：**Mate 技术人员会分析并纠正所有可能的误报。
- **误挡回报：**使用方便的提交工具，在遇到被错误标识的邮件时，

Mate 的用户社群（大量使用者账户可以尽快地通知 Mate。

新型未知恶意 APT 邮件防御技术

Mate Email UTM 产品，在原有的邮件安全防御基础之上专门针对 APT 新型邮件威胁，加入的全新的 APT 威胁检测模块；可以在放病毒引擎识别，垃圾邮件检测之后，再对未知的恶意邮件和附件进行云端沙箱的主动的行为特征分析，

- **APT 静态特征对比**
  通过 MateCloud 全球防御中心收集和更新的最新的威胁情报资讯 TID(Threat Intelligence Database)做快速判断对比，包括最新的 C&C 僵尸网络 IP address、domain name、URL 链接等
- **云端沙箱 SandBox 动态扫描系统**
  透過 Mate 深层检测 DI (Deep Inspection)引擎会将邮件头(Header) 正文(Body) 附件(Attached files) 做分解分析,侦测后会将其中包含的 URL 链接 或 带有特定附件的可疑文件打包加密发送到 MateCloud 通过强大的云端沙箱进行全系统模拟 (Full-system emulation)分析技术,可在 3~10 分钟之内触发和诱捕潜伏的恶意程序或代码现出原形，同时配合关联式的行为分析引擎，对恶意程序行为做威胁等级判断，在返回识别结果到客户端部署的 Mate 设备对该邮件进行隔离或放行；
- **MateCloud 云端沙箱可模拟丰富的系统环境进行全面识别**
  MateCloud 云端沙箱可以模拟多种常见的桌面操作和移动设备操作系统，对新的未知恶意程序在各种系统平台下的恶意行为都会做全面的扫描和监控



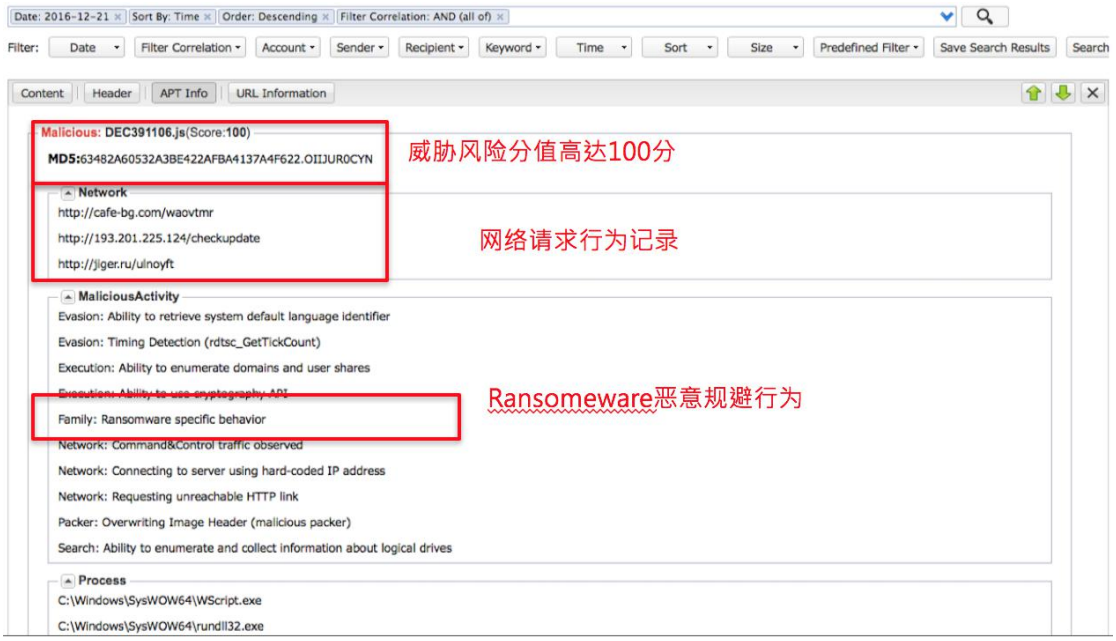
- **邮件内容检测深度**

- 针对 APT 邮件攻击与变种 Malware 威胁的全新 APT 邮件防御模块 ，可安装于现有 Mate Email UTM 或 Anti-spam Gateway 系列产品中。
- 全新一代的动态分析砂箱
- 执行二进制文件，存取网页，开启文件
- 监控并且分类观察到的行为
- CPU 模拟环境 (CPU emulation)
- 能看到恶意软件所执行的每个 CPU 指令集,而不仅止于系统呼叫
- 提供大幅提升的能见度
- 附档作拆解并做深层检测 ，可有效地侦测并拦截 APT 邮件及 Malware 的威胁

Mate APT 产品功能

对于云端沙箱分析检测出来的 APT 恶意邮件，Mate 邮件安全网关系统会将其单独隔离存放在 APT 邮件区，可以供管理员检查，分析其邮件所包含的具体内容；

对于每一封因为侦测到 ATP 深度威胁而被拦截的邮件，都会显示完整的恶意行为分析报告，管理员通过点击该封邮件的 APT 信息就可以查看到该恶意邮件所包含的所有异常恶意行为记录，包括：网络请求，下载文件，执行进程列表，调用系统危险 API 列表，注册表修改 等等具有非法危险操作的行为报告；



邮件内容策略控管

Mate Email UTM 包括多项邮件内容策略控管功能。当与邮件策略功能一起使用时，内容策略一致性功能使得管理员可以实施公司的电子邮件策略，减少法律责任，并确保符合法规要求。Mate Email UTM 邮件政策功能提供以下企业需求：

- **内容层级过滤(Content Level Filtering)：**可以针对邮件的标头(Header)、主旨(Subject)、内文(body)、附件文件(attachments)文件名及附件文件内文(支持 txt, rtf, doc, pdf, xls, ppt,)的过滤。
- **自行定义邮件政策：**弹性的定义过滤范围(Inbound and/or outbound)、寄件人(Sender), 收件人 (Recipient), 敏感的关键词(keyword)、MIME 类型、档案大小、档案格式、及时间排程等等。
- **关键词管理：**管理员可定义多笔关键词(支持 Double-Byte)，用以检查邮件内容与附件内容是否违反公司政策或是使用规定。
- **附件管理：**管理员可以扫描具有特定属性（例如，扩展名、文件名、MIME 类型、大小等）的附件，并执行特定的操作。 例如，您可以隔离所有 ZIP 文件，删除图像文件或过滤掉过大的邮件。
- **时间管理：**管理员可以根据时间来定义何实执行策略。例如可以定义上班时间不可以寄送大量图片的信件，以避免对外频宽用尽。
- **简单的邮件策略控管画面：**一个简单易用的图形接口，使您能够快速建立公司邮件策略。可以快速启动和停用个别邮件策略，显示启动状态并选择邮件策略运行的顺序。

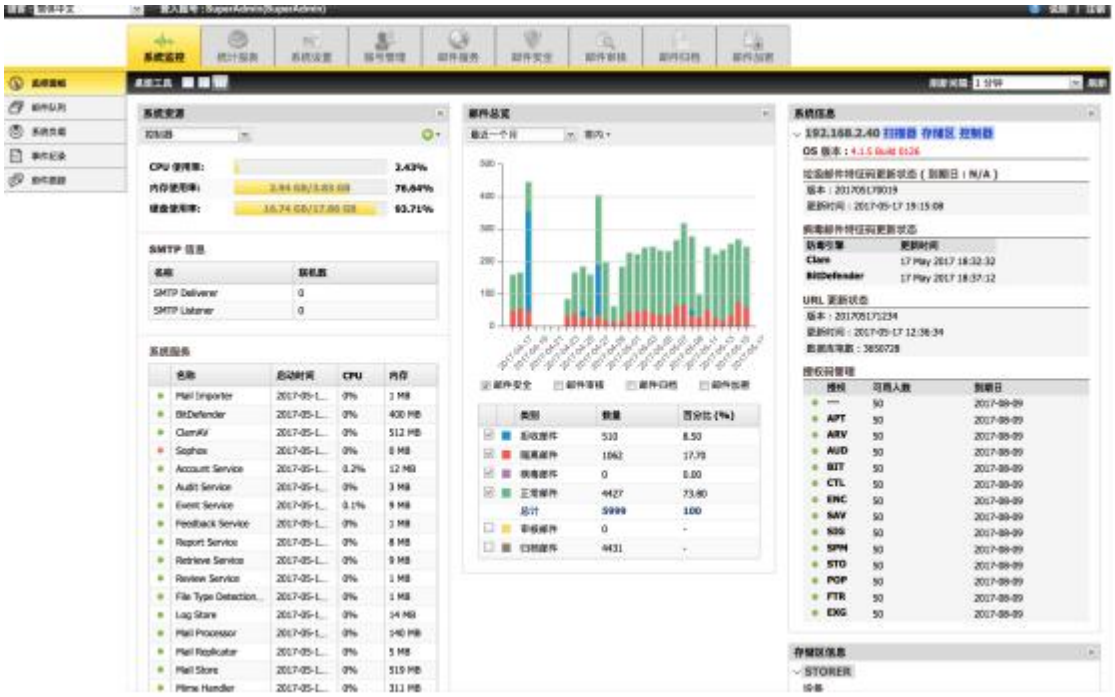
- **多个条件：**您可以使用不同条件的多个组合来编写复杂的规则，并根据内容、标头、MIME 类型和多个其它条件进行扫描。 您可以在内容过滤中建立的条件的数目没有限制。
- **多项操作：**对于与内容过滤相匹配的邮件，管理员可以选择将其删除，转发到某个电子邮件地址，对其进行修改或执行其它操作。

群组策略功能

Mate Email UTM 系列设备允许您为群组建立不同策略。 可以通过 LDAP 汇入公司内部所有人员和群组。群组策略定义使邮件处理的自定义过程具有了最大的灵活性，包含可以定义组策略的成员资格，并选择它使用的过滤策略；也可以为每个群组套用不同的内容过滤处理方式，并且设置群组的黑白名单。

终端用户功能

Mate Email UTM 系列设备可以让妆端用户能够管理和自定义他们的过滤功能。用户可以登录到控制中心的特殊部分并选择适当的设置。



可自定义的最终用户功能包括：

- **黑名单：**用户可以指定将始终禁止的地址。 这些项可补充管理员在组织范围内定义的禁止的发件人列表。
- **白名单：**用户可以指定允许忽略反垃圾邮件过滤的发件人。
- **语言设置：**用户可以指定他们通知信语言格式。
- **回报原厂：**用户可以将错过的垃圾邮件或误报提交给 Mate 进行分析。
- **终端用户隔离区：**网络上的用户随时可以登录到他们自己的隔离区并查看他们被隔离的邮件。
- **隔离区邮件搜索：**用户可以使用多个条件搜索隔离区中的邮件，这些条件包括寄件者、收件者、主旨、关键词、时间范围。

管理功能

Mate Email UTM 系列设备的特点是自动内容更新以实现全面防护。它们还具有非常丰富的功能和充分的可定制性，使管理员能够控制和了解组织内的电子邮件安全问题。管理功能的范围包括：

- **Web 管理接口：**Web 接口的管理控制中心使管理员能够使用 Web 浏览器来查看综合过滤性能的实时操作画面。
- **自动过滤器下载和统计信息传输：**从客户端进行安全 HTTPS 进行更新过滤器的下载。 该同一过程还会将统计信息从客户端传输给 Mate，以便 Mate 评估部署的过滤器的性能和有效性。 该过程无需管理员干预，而且在更新过程中过滤器永远不会停止。
- **支持多位管理员：**建立其它管理员账户，授予每个管理员管理 Mate Email UTM 不同功能组件所需的管理权限级别。
- **自动电子邮件警报：**Mate Email UTM 可以选择当出现以下任一情况时向系统管理员发送警报：
  - ✓ 某件组件不响应或不工作。
  - ✓ 反垃圾邮件过滤器更新日期过期。
  - ✓ 防病毒过滤器过期
  - ✓ 可用的磁盘空间少于指定的数量。
  - ✓ 反垃圾邮件授权已过期。
  - ✓ 软件更新授权已过期。
- **综合事件纪录：**详细的事件纪录让管理员可以方便找到问题。

其它更多的管理功能尚包括：

- **回报分析**：由管理员和用户标示漏拦垃圾邮件或误档正常邮件发送给 Mate Global Antispam Center 进行分析。
- **安全级别**：支持 TLS（传输层安全性，SSL 的后续协议）加密。
- **隔离区**：Mate Email UTM 系列提供了 Web 管理接口的隔离区。管理员可以登录并查看 Mate Email UTM 软件为其组织中的所有用户隔离的垃圾邮件。隔离区功能的范围包括：
  - ✓ 电子邮件通知：隔离区可以向用户发送定期隔离垃圾信通知，其中列出新隔离的垃圾邮件，使用户可以立即将邮件释放到他们的收件箱或登录到他们的个人隔离区。
  - ✓ 通过一次单击释放隔离的邮件：垃圾邮件隔离区摘要的收件人可以单击链接来立即释放或查看捕获的垃圾邮件，而无需登录到个人隔离区。
  - ✓ 隔离区邮件搜索：用户和管理员可以使用多个条件搜索隔离区中的邮件，这些条件包括：To: 标头、From: 标头、邮件正文、Subject 和时间范围。
  - ✓ 可自定义的通知模板：管理员可以自定义发送频率、邮件内容和内容类型（HTML、文本或两者）。 他们还可以指定摘要是否包括嵌入的视图邮件并发布邮件链接，以便用户无须登录即可访问邮件；还可以选择是否将摘要发送给分发列表。
- **报告**：Mate Email UTM 系列包括丰富的报告功能，其中包括：
  - ✓ 综合报告：查看所有作为 Gateway 运行的 Mate Email UTM 系列设备的综合过滤性能统计数据。
  - ✓ 多个预设报告：使用多个不同类型的预设报告来提供过滤性能和电子邮件攻击的全面实时报告。
  - ✓ 报告汇出：汇出报告数据，以便在任何报告或电子表格软件中使用以供进一步分析。
  - ✓ 报告调度：调度有关电子邮件的生成和发送的报告。

邮件备份功能

Mate Email UTM 系列设备的特点除了针对邮件提供防护外，还可备份正常邮件在此设备上。透过自有的 index 技术，可以在成千上万的邮件资料中找到需要的邮件，主要特色如下：

- **Web 管理接口**：基于 Web 的控制中心使管理员以及终端用户能够使用 Web 浏览器来查看综合过滤性能的实时操作画面。

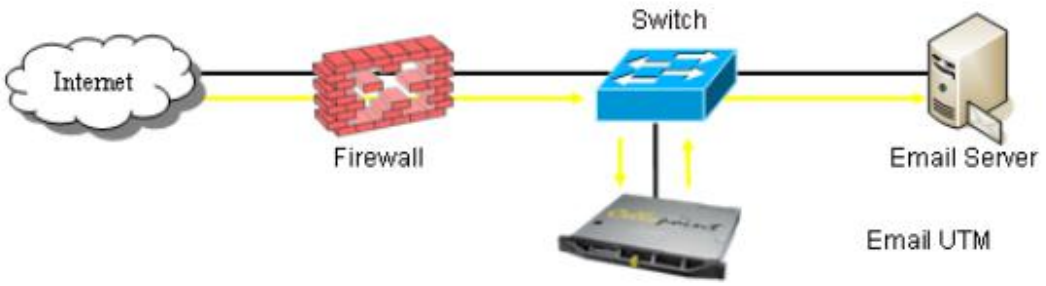
- **建立索引：**针对邮件内容以及附件内容建立索引，方便用户找到想要的数据。
- **关键词提示：**标示出关键词在邮件哪些部份
- **邮件还原：**提供邮件还原功能，若使用者不小心删除邮件，可以透过 Mate Email UTM 将信件重送至信箱。
- **BCC 收件人显示：**可显示信件之密件副本收件人。
- **储存装置管理自动电子邮件警报：**当储存装置发生故障时，可以电子邮件方式通知指定之管理者。

部署模型

客户可以采用两种模式部署 Mate Email UTM 系列设备，包含网**关模式（Relay Mode）**与**透通模式（Transparent Mode）**。

■ **基本网关部署**

这是建议的部署模型。Mate Email UTM 系列设备位于最外面的网关层，它处理入站、出站邮件，提供安全电子邮件服务，以及将邮件中继到其它中继层或面向用户的邮件存储层。下图显示了部署在防火墙后、网关处的 Mate Email UTM 系列设备。



优点

- 由于垃圾邮件来自外界，因此网关是部署 Mate Email UTM 系列设备的合理有效位置。
- 靠近网关部署设备时，经过电子邮件防火墙的过滤，可以最大限度地降低邮件处理和硬盘储存需求以及网络频宽。

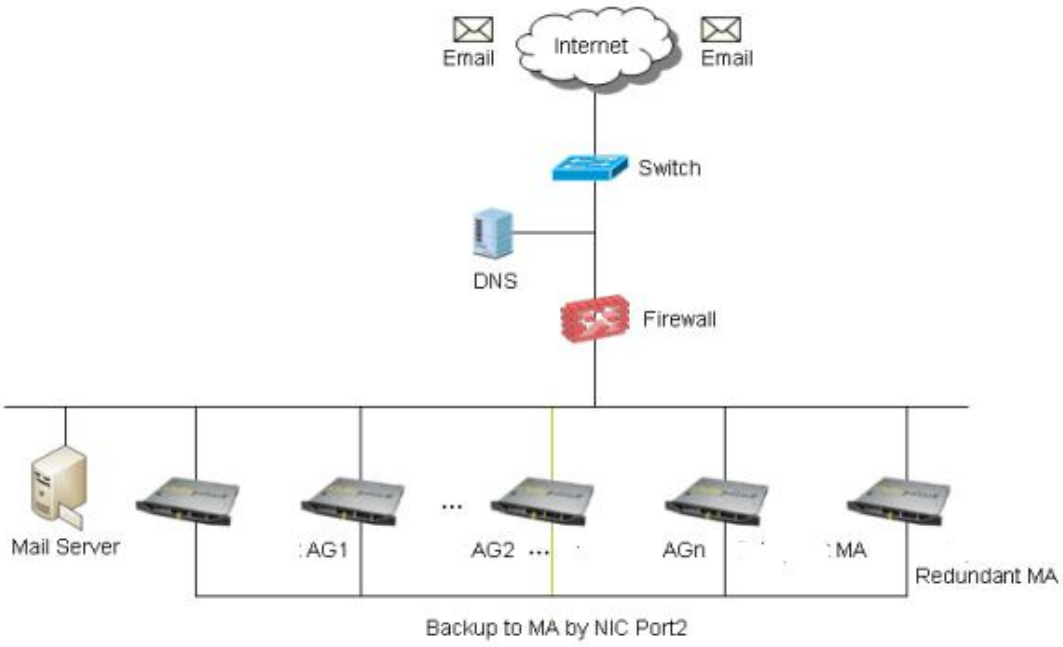
注意事项

- 运用此模式布署 Mate Email UTM，必须要搭配设定。

◆ 有些小型组织没有专用网关服务器或网关层。与之相反，他们将网关服务器和内部邮件服务器部署在同一台计算机上。

■ **网关部署 - 多个设备**

下图显示了一种网关部署，该部署使用一台 Mate Email UTM Mail Reporter 系列设备的控制中心管理网络设备上的多个 Mate Email UTM Mail Gateway。



优点

◆ 利用防火墙内或防火墙与 Scanner 之间的 SLB，该方法可以使负载均衡地分布于多个 Gateway 上。

◆ 该模型将 Gateway 与 Reporter 之间的功能完全分开。这种功能的可取之处在于：有更多的资源可供在 Gateway 上处理邮件时使用，并且可避免遭受因控制中心停机所造成的邮件服务损失。

Mate 解决方案的效益

根据目前的各项统计数据都一再显示，垃圾邮件，病毒邮件，以及新型 APT 威胁邮件的数量是以倍数的方式向上成长；而不管对个人或者企业组织而言，电子邮件上面传输的信息只会越来越重要；邮件安全相关议题，例如垃圾邮件、邮件攻击、邮件诈骗等，也均已经列为各信息部门的重要工作项目之一，因此如何选购与建置有效的邮件安全防御机制绝对是刻不容缓的议题。

Mate 邮件安全解决方案将防御机制建置于 MateCloud™云端架构下，在云端架构下透过独特的寄件者信誉评等、威胁感知系统、动态 APT 沙箱系统与 Mate 全球防御中心 7x24 的监控机制等，可快速且有效地阻挡日益增加的垃圾邮件、病毒、钓鱼邮件、APT 邮件、间谍程序与邮件炸弹等威胁于企业组织之外，让企业组织有效做好邮件安全防护，以提升产业竞争力。

综合以上所述，整理导入 Mate 邮件安全解决方案可获取以下效益：

- **解决日趋严重的垃圾邮件问题**

Mate 邮件安全解决方案透过云端机制，能够快速且实时地布建最新垃圾邮件防御特征数据库至客户端，能够以最实时的方式拦截各类型垃圾邮件，以确保企业组织免于垃圾邮件的困扰。

- **4 层有效防御体系过滤和拦截病毒以及恶意 APT 威胁邮件**

Mate 邮件网关通过搭配最多三层的专业放病毒引擎，可以在第一层优先静态识别大量的已知恶意邮件和病毒邮件，然后配合 MateCloud 的全球恶意邮件发送 IP 地址信誉数据库可以进行第二层的恶意邮件来源识别；再通过云端垃圾邮件特征收录的各种已经散布发现的恶意邮件样本特征，通过垃圾邮件特征库的及时发布，可以有效居于邮件内容特征实现第三层的邮件安全防御；最后搭配 MateCloud 先进的新一代云端 SandBox 技术，实现第四层的全面邮件安全防御体系，让无论是已知的恶意邮件威胁，还是针对性的未知 APT 渗透式邮件威胁，统统无处遁形，全面防护企业的电子邮件环境安全；避免再因遭受类似勒索病毒，钓鱼邮件等类型的邮件攻击所带来的损失。

- **确保使用者不会遗漏重要邮件**

Mate 邮件安全解决方案可自动将垃圾邮件、病毒邮件隔离在 Mate Email UTM 设备上，同时于固定时间寄发隔离通知信，以主旨条列方式清楚地告知使用者被隔离的垃圾邮件，确保使用者不会遗漏重要邮件。

关于 Mate

Mate 由一群业界经验丰富的领导团队及优秀研发人才于 2003 年所创立。我们以客户的需求与前瞻的产品设计概念，为世界各地合作伙伴与客户开发创新的解决方案与服务模式。Mate 专注于邮件安全与管理的议题，全心投入研发，提供 MateCloud™云安全防御、归档检索与网格存储、内容过滤稽核、效能优化、负载平衡解决方案。协助电子邮件系统管理者解决安全威胁、数据膨胀、机密外泄、效能不佳及中断服务等问题。

愿景(Vision)

成为电子邮件安全与管理领域中最受信赖的公司

使命 (Mission)

我们的使命是提供客户最佳的产品与服务，将邮件安全与管理的范围拓展至企业、组织、ISP 与云服务供货商。同时为合作伙伴创造利润与提供销售利器、为股东创造卓越的投资报酬率、为员工创造良好的发展环境与实现梦想。

自我期许

不断成长 – Mate 提供弹性的产品组合方式，紧紧把握产业脉动，挖掘新的商机。我们致力于加速邮件安全、内容稽核与法规遵循、归档检索及防止数据外泄等方面的业务成长。技术与策略合作伙伴关系可协助我们开拓新业务，藉此巩固我们的市场地位，同时做为成长的驱动力。

持续创新 – 包括创新理念、技术研发及管理，让我们的产品与服务推陈出新，以提供完整的邮件安全与管理解决方案，如防垃圾邮件、网络钓鱼防护、内容稽核、归档检索、数据外泄防护以及遵从法规的功能。我们发展全新的电子邮件云安全技术，让客户免于遭受日新月异的安全威胁侵害。

产品与服务

Mate 是提供邮件安全防御、内容稽核与归档管理解决方案的领导厂商，协助企业组织、学校、区网中心、金融保险、政府机关及服务运营商保护并管理其邮件数字资产。随着邮件威胁攻击趋势的不断演变及客户环境的变化，我们投入研发资源于虚拟化与云安全服务领域，希望协助客户减少成本与简化管理复杂性。

Mate 运用内部研发成果以及所属 MateLabsTM 的创新技术，我们将新的技术搭配核心解决方案，提供弹性的解决方案来因应客户不断演变的需求。

产品线：

- Email UTM 整合式邮件安全与管理方案
- Anti-spam Gateway 反垃圾邮件网关
- Auditing Appliance 邮件稽核平台
- Mail Archiver 邮件归档检索平台
- Digital Signature 邮件数字签名