魔盾邮件安全产品

产品白皮书

产品版本：V5.0

文档版本：V1.0

日期：2024 年 11 月 19 日

版权声明

免责声明

本文档仅提供阶段性信息，所含内容可根据产品的实际情况随时更新，恕不另行通知。如因文档使用不当造成的直接或间接损失，本公司不承担任何责任。

文档更新

本文档由北京魔盾信息科技有限公司于 2024 年 11 月最后修订。

联系我们

北京魔盾信息科技有限公司

网站：https://www.maldun.net

销售咨询/技术支持电话：4008062826

文档修订记录

版本	修改日期	修改人员	修改记录
V1.0	2024.11.19	黄旭	创建文档

文档审核记录

版本	审核日期	审核人员	审核记录
V1.0	-	-	创建文档

目 录

一、概述

1.1 魔盾邮件安全解决方案简介

魔盾邮件安全高级防护系统是魔盾安全开发的用于应对邮件全生命周期威胁的邮件安全产品组合。

魔盾邮件安全高级防护系统由魔盾邮件安全网关、魔盾文件分析沙箱、魔盾链接分析沙箱及魔盾集群中控平台系统等产品组合而成。企业可根据自身实际情况灵活选择各产品的部署形态、部署方式并进行组合。

魔盾邮件安全高级防护系统以下一代邮件安全架构为基础，在传统邮件安全基于特征的静态分析的基础上，融入了基于威胁、行为的动态分析技术，可为企业的邮件安全提供多维度、深层次并可应对多种邮件安全威胁的邮件安全整体解决方案。

1.2 赋能综合威胁防御能力

区别于其他邮件安全解决方案，魔盾邮件安全解决方案基于先进、独特且强适应性的邮件工作流引擎基座，构筑出不断进化、持续学习、主动更新、基于 AI 的邮件全生命周期威胁防护平台。在邮件安全威胁不断变化的现状下，魔盾邮件安全解决方案可为企业提供适应邮件安全大环境的邮件安全防护能力，让邮件安全防护更简单、更稳定、更高效。

1.3 简化策略与管理工作

当前市场上的邮件安全产品解决方案，需要企业运维人员付出大量的时间和精力对安全策略进行手动的配置更新。魔盾邮件安全解决方案得益于自研的“自适应智能引擎的自动过滤更新”及“人工智能助手”技术，无需企业运维人员的人工干预。在“Hands-Off（自托管）”模式下，产品可自学习和适应企业邮件环境，并根据学习结果智能调整邮件安全相关策略。除“自托管”模式外，企业也可根据邮件业务实际情况，手动配置邮件过滤及细颗粒度的邮件安全策略。

1.4 魔盾邮件安全解决方案部署

通过部署魔盾邮件安全解决方案，用户可以保护现有的网络与系统基础设施，包括邮件服务器与邮件存储系统。在许多情况下魔盾邮件安全解决方案可以高效过滤掉 99.9%以上的问题邮件流量，以减轻过载的企业内部系统负担。魔盾邮件安全解决方案也可以与第三方产品集成，通过综合防御的形式确保最终用户的安全。

1.5 魔盾邮件安全解决方案优势

魔盾邮件安全解决方案基于垃圾邮件内容识别规则、威胁情报加持的信誉过滤系统、高级威胁行为实时检测防护及其他下一代邮件安全平台的威胁分析功能，可为企业运维及安全管理员提供更轻量、更智能、更易用的邮件安全威胁分析及管理平台。

二、邮件安全威胁

2.1 邮件安全威胁概述

信息时代，电子邮件在人们的工作与生活中仍扮演着极为重要的角色。2023 年全世界平均每天的商务电子邮件超过 2000 亿封，电子邮件通常是企业信息与业务沟通的主要工具。企业进行业务往来依赖于邮件系统的正常运转，邮件系统的安全以及邮件所传递信息与内容的管理也变得极为重要。在不同的网络与邮件传递环境中快速发送和接收电子邮件的能力是企业业务和个人沟通的核心。由于电子邮件的重要作用，恶意攻击者花费了大量的时间和精力来颠覆电子邮件，以达到他们想要的用法。从过量的不需要的邮件到包含危险内容的邮件，新的电子邮件威胁不断出现。

对于大多数企业或组织来说，电子邮件是内部和外部沟通中最为关键的一个渠道。然而全球超过 50%的电子邮件流量是垃圾邮件，垃圾邮件显著影响了业务效率。极速增长的通过电子邮件传播的威胁，包括网络钓鱼，钓鲸，欺诈，勒索，APT 等在世界范围内造成了巨大的破坏，对商业运营造成不可估量的损失。企业邮件管理员及安全工程师正在面临的问题是如何应对这些不断升级的安全威胁并保持邮件本身的信息价值。企业与组织除了需要基本的反垃圾邮件的功能外，越来越需要集成安全内容和威胁管理的解决方案，以切实有效的应对伴随电子邮件而来的多种威胁。

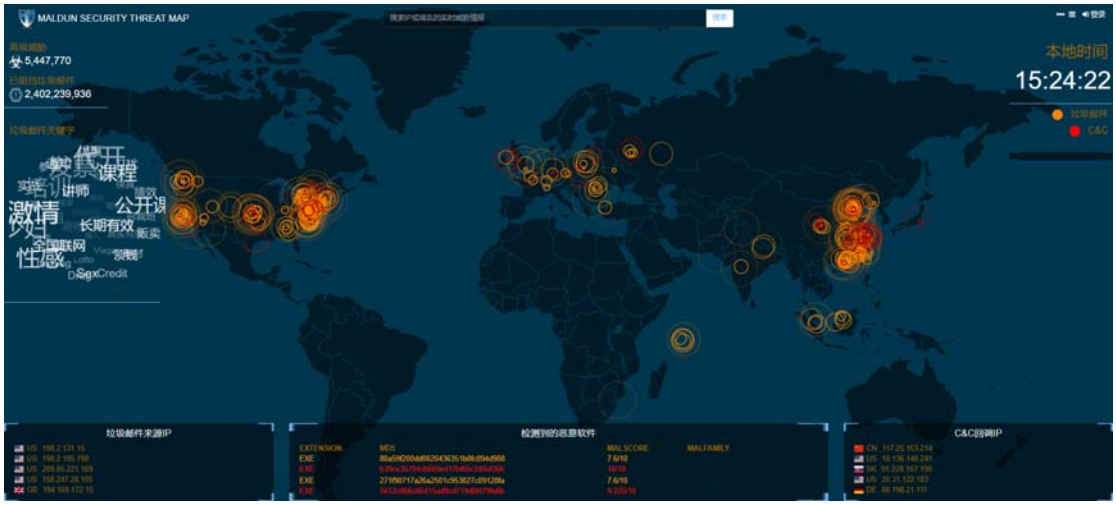

图 2-1 魔盾安全威胁展示地图（全球视图）

2.2 邮件安全风险

作为外部数据进入企业的主要入口之一，企业邮件系统不断遭到病毒程序、垃圾邮件、非法内容及高级针对性威胁的侵犯和攻击。这类邮件会干扰企业正常运作，影响邮件系统内的正常业务邮件的投递；恶意文件/URL 链接等进入到的用户邮箱后，会对用户的信息造成安全隐患。此外，这类邮件威胁可能引发企业机密信息的泄露，损害企业的品牌与声誉，甚至导致企业陷入法律纠纷。因此，邮件安全成为企业安全防护中极为重要的环节。

早期的邮件安全威胁通常为纯文本内容的垃圾邮件，有比较明显的垃圾邮件特征和相对单一的目的，可以使用特定的关键词组合进行有效过滤。

然而随着恶意邮件攻击方式的不断演化，最新的恶意邮件已经包含了相当复杂的技术，包括邮件主题/正文等内容的高度随机化、大量的内容填充、发件服务器的动态跳转和隐藏，以及使用发件地址伪装等反过滤技术；同时通过邮件攻击的主要目的已经由信息传播转换为经济利益，通过钓鱼、信息盗取、加密勒索等攻击形式，获取惊人的收益。

2.3 主要邮件威胁

当攻击者发送的垃圾邮件或包含恶意文件/URL 链接的邮件进入到企业用户的邮件系统时会带来不同的风险或问题，如：用户个人信息被盗取导致财产损失、用户电脑遭受恶意文件攻击导致电脑无法使用的同时，文件的横向扩散会导致引发大规模的恶意攻击事件、用户文件被加密导致无法正常办公等。这些问题不仅影响用户个人，也会对企业业务的正常运作带来不可估量的影响。

通常所说的垃圾邮件是指未经企业主动请求或许可，强行、大批量发送到企业所有/特定用户邮箱中的任何电子邮件，如：UBE (Unsolicited Bulk Email)-垃圾邮件、UCE (Unsolicited Commercial Email)-未经请求的商业电子邮件。恶意邮件则包含了所有收件用户不愿收到的或可能对收件用户系统产生危害的电子邮件，因此人们常以恶意邮件指代所有的邮件威胁。

邮件安全威胁的常见特征为：随机生成或伪装的发件人及发件地址（如：官方机构、银行或公司内部财务、人力、总经理、董事会等）、收发件人之间没有任何可识别的关系 、邮件内容有明显的语法错误、邮件内容具有欺骗性或误导性等。此外，邮件安全威胁还包含恶意或未知其安全情况的 URL 链接或附件文件。在用户点击链接或打开附件文件时，相应程序会入侵用户电脑并将威胁渗透进企业网络及内部各个业务系统。

垃圾邮件、恶意邮件和其他形式的非必要邮件投递占据了企业电子邮件投递量整体的 50%以上，因此企业的邮件系统以及现有的邮件安全网关产品必须有一定的性能冗余对此类邮件的分析识别及处理，同时企业的运维人员、安全人员随时需要对邮件系统/传统邮件安全网关产品漏拦的邮件进行手动的维护。

如果由企业用户查看并判断所有收到的邮件，他们很快会被大量的垃圾邮件、恶意邮件的信息所淹没，浪费大量的时间用于邮件的筛选。

感染用户系统的病毒与其他形式的通过邮件传递的恶意软件，是另外一个邮件威胁的主要关注点。据分析 67%的恶意软件通过电子邮件附件传播，它们可能危及企业用户电脑或业务系统的安全，或者用户个人信息可能被直接窃取。被感染的系统资源可能被利用作为僵尸网络的一部分触发额外的攻击或发送大量的恶意邮件。

钓鱼和鱼叉式钓鱼威胁则诱使用户泄露个人信息。这样的邮件看起来好像来源于可信的地址，通常是与用户有关系的人或组织。当用户成为钓鱼邮件的牺牲品时，企业、企业用户个人个人和企业财务信息可能被无意中泄露，造成重大经济损失或身份盗窃。钓鱼邮件与病毒邮件每年给企业平均造成超过 25 万元的经济损失。

2.4 邮件高级威胁

针对企业和组织的网络威胁正在不断演变。攻击者的目的不再仅仅是感染和破坏。在过去的几年中，网络威胁变得更加复杂和持续。这些攻击背后的动机越来越与经济或政治相关，并可能对受害者产生严重的影响，例如伪造发件人攻击（Spoofing，或 Business Email Compromise，简称 BEC）、高级持续性威胁、勒索软件等。

伪造发件人邮件攻击是指，有人在“发件人”一栏写入自己并没有准入权的邮箱地址（可能是虚假地址），来掩盖自己的真实邮箱地址。这样做是要让收

件人误以为邮件来自所在企业的同事或高管，并冒充发件人向收件人索取敏感信息，发布威胁指示等。

高级持续性威胁（APT）和勒索软件对企业来说尤其危险，因为黑客攻击性强、攻击手段极其复杂、而后果又极为严重。这些攻击利用了网络钓鱼或零日漏洞，并且常常绕过基于静态签名的传统反病毒解决方案。企业与组织需要的不仅仅是阻止威胁，而必须了解追踪威胁，如：谁在进攻、攻击是如何开始的、如何防守等。

三、魔盾邮件安全解决方案

魔盾邮件安全高级防护系统是魔盾安全开发的用于应对邮件全生命周期威胁的邮件安全产品组合。魔盾邮件安全高级防护系统由魔盾邮件安全网关、魔盾文件分析沙箱、魔盾链接分析沙箱及魔盾集群中控平台系统等产品组合而成。企业可根据自身实际情况灵活选择各产品的部署形态、部署方式并进行组合。魔盾邮件安全高级防护系统以下一代邮件安全架构为基础，在传统邮件安全基于特征的静态分析的基础上，融入了基于威胁、行为的动态分析技术，可为企业的邮件安全提供多维度、深层次并可应对多种邮件安全威胁的邮件安全整体解决方案。

魔盾邮件安全网关是一个多功能的邮件网关，可部署在互联网与企业邮件服务器之间，提供出站/入站电子邮件安全防护能力。魔盾邮件安全网关系统的下一代电子邮件安全架构可过滤各种邮件安全威胁，例如垃圾邮件、病毒邮

件、钓鱼邮件、诈骗邮件、灰色/广告邮件等。魔盾邮件安全网关系统可与魔盾文件分析沙箱、魔盾链接分析沙箱等产品集成，能够检测分析并阻止高级威胁或未知威胁的邮件进入到企业的邮件系统。

魔盾邮件安全网关的产品结构如下图：

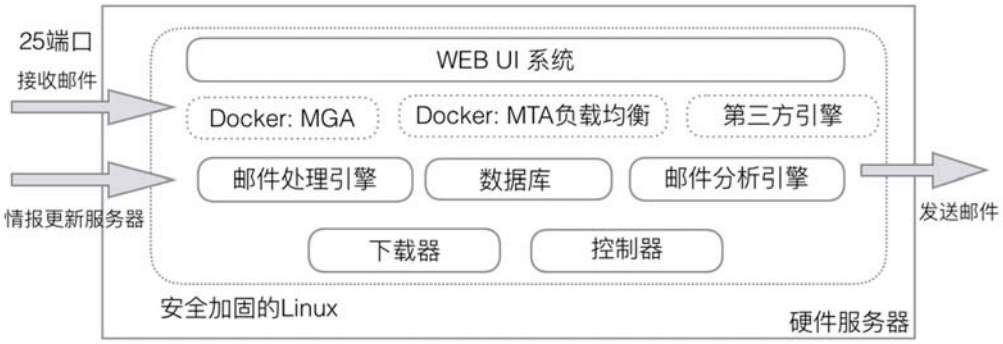

图 3-1 魔盾邮件安全网关架构简图

魔盾邮件安全网关通过接收魔盾邮件威胁情报中心的情报与规则更新，保持对邮件安全威胁的持续检测能力。魔盾邮件威胁情报中心是一个 24X7 运行的邮件威胁数据采集、分析与处理中心，通过机器学习和分析人员对邮件数据的人工分析，生成最新的关于邮件威胁的情报与规则，并实时更新到魔盾邮件安全产品。

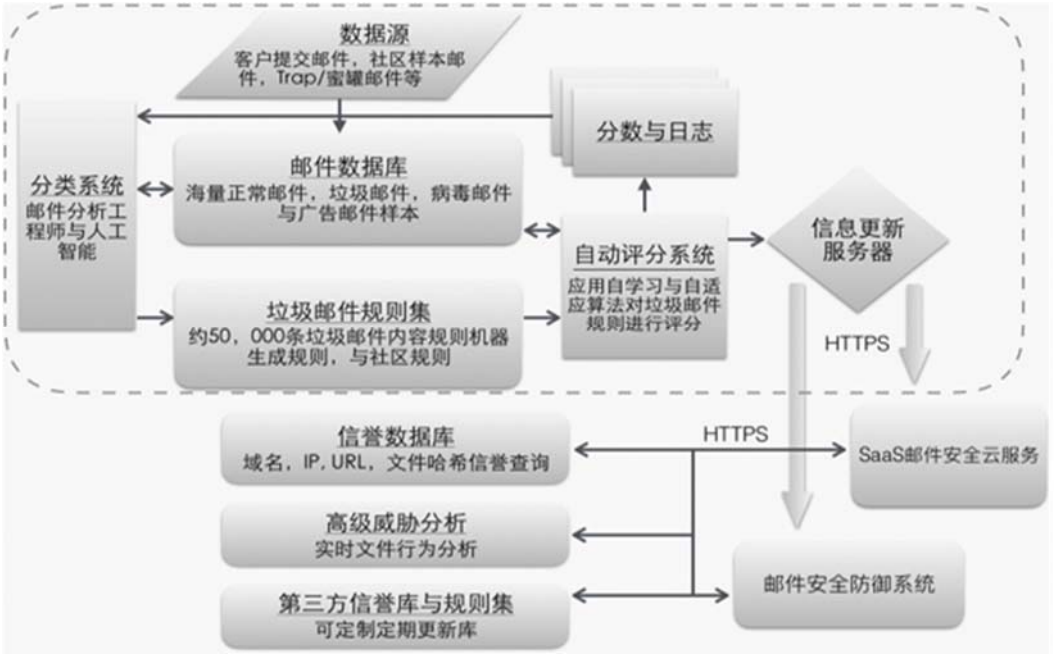

图 3-2 魔盾邮件安全情报更新架构图

3.1 一站式解决方案

魔盾邮件安全网关是一款功能完备的一站式多功能网关设备。魔盾邮件安全网关设备集成了核心硬件和软件，以提供全面的、安全的、易于部署的邮件信息安全解决方案。这些元素包括：

- 硬件：魔盾邮件安全网关支持在 Intel X86 及国产化 X86 架构的服务器上运行；
- 软件： 魔盾邮件安全网关预装定制化的 Linux ®操作系统。此外，系统内还提供了邮件分析引擎和与管理平台模块，包括各种插件和所有必要的邮件传输代理（MTA），保证与外界的和企业内部邮件服务器的邮件传递。魔盾邮件安全网关的软件更新简单易用，可确保安全更新的最小中断时间。

- 安全配置： 为了应对电子邮件服务器直接暴露在互联网上的风险，魔盾邮件安全网关通过了一系列安全平台的技术支持。嵌入的操作系统包括了内核锁定及对常见漏洞和攻击的预处理措施。例如，为了防止黑客的攻击，只包含最重要的服务，所有不必要的端口都被关闭。同样，魔盾邮件安全网关所提供的邮件投递功能被安全加固以阻止非授权的邮件传递。内置的邮件安全管理平台的管理和控制功能也受到可选的基于 Web 的身份验证的保护，只允许组织内的授权用户访问。

- 情报更新： 为了确保对最新电子邮件威胁的全面保护，邮件安全防御不断实时强化与自动更新来自魔盾的邮件威胁情报、反垃圾邮件过滤规则和防病毒特征库。魔盾邮件安全网关可以设置自动执行所有过滤器和分析引擎的更新，以缓解管理员的负担。引擎更新下载过程包含了严格的验证以保证更新的规则和特征库来自魔盾更新服务器。即使设备正在接收更新，邮件分析引擎仍在工作，因此即使在更新期间邮件安全也可以得到完全保护。需要注意的是，由于魔盾邮件安全产品序列号过期而导致魔盾邮件安全产品更新服务验证失败时，魔盾邮件安全产品将停止情报更新。此时魔盾邮件安全产品仍将继续工作，而不会影响用户邮件传递。但是由于无法获取最新的邮件威胁情报、反垃圾邮件规则和反病毒规则等，魔盾邮件安全产品的威胁检测能力将会有超过 10%的下降并随时间逐渐增加，客户可能会受到新型邮件威胁的攻击而无法受到保护。我们建议用户对情报更新服务有效期保持关注，确保序列号在有效期范围内以获得完整及时的邮件防护。

3.2 邮件安全管理

魔盾邮件安全网关可用于在一个节点内执行多种功能。对于较小规模的安装部署，管理员可以配置单一的设备来执行所有需要的功能。较大规模的安装通常选择部署多个网关设备和一个/多个专用的集群中控平台来执行集中管理功能。可用的设备包含:

- 魔盾邮件安全网关（专用）：只进行邮件过滤和邮件传递。管理员可以设置一个或多个邮件安全网关。当需要多个魔盾邮件安全网关设备实现负载均衡和高可用性目的时，多个邮件安全网关设备可以被配置为使用 DNS 轮循和加权的 MX 记录进行区分。

- 魔盾集群中控平台（专用）： 魔盾集群中控平台（CSM）可以管理多个邮件安全网关设备，并支持集中管理垃圾邮件、可疑附件隔离以及合规事件的存储及查看。CSM 负责多邮件安全网关设备的集中报告、策略管理和消息跟踪等功能。

极端情况下，当集群中控平台出现故障时，集群内的邮件安全网关设备仍可保持关键的邮件过滤和投递功能；集群中控平台内的邮件安全网关集群也可轻易完成扩展。

3.3 高级威胁防护

魔盾文件分析沙箱（ATP）使企业能够检测邮件附件内可能含有的「有针对性的攻击和威胁」，并将威胁信息转化为即时的行动和保护。魔盾文件分析沙箱结合深入的静态分析、动态分析（恶意软件的沙盒）和机器学习来实现高级

或未知威胁检测，如零日漏洞攻击等。不同于传统的沙箱，魔盾文件分析沙箱集成了额外的实时检测能力，以触发威胁行为和提升检测效果。随着机器学习技术的引入，魔盾文件分析沙箱可将具有相似性的威胁集群起来，以检测未知的威胁并进行分类。

魔盾文件分析沙箱（ATP）与魔盾邮件安全网关无缝结合以实现高级威胁的检测和分析。魔盾文件分析沙箱使用创新、分层的方法检测已知和未知的威胁。它结合了优化的静态分析引擎，包括文件属性、代码分析、病毒签名、声誉等数据，以及动态分析的实时虚拟执行（沙盒）对可控环境中的实际行为。魔盾文件分析沙箱还可以进行内存分析、实时网络流量以及衍生文件分析。通过实时触发和相关性分析，魔盾 ATP 可以检测到深度隐藏的威胁。

3.4 出入站邮件处理

魔盾邮件安全网关通常部署在企业网络的出口，负责处理接收和发送电子邮件。做为核心的邮件通信平台，魔盾邮件安全网关包含了强大高效的 MTA 解决方案，以保证高性能、高安全性和灵活性。魔盾邮件安全网关支持企业内部邮件多域名的差异化管理，还可针对不同域名，用户组，用户单独配置邮件路由和邮件安全策略。

如下图所示，通过魔盾邮件安全网关的邮件经过若干处理层和过滤模块后才会继续投递进程。这些处理包括基于发件人验证&连接 IP 声誉及 SMTP 连接有效性的连接控制检查、用户黑白名单、全局发件域名与发件地址白名单、基于邮件特征的自定义规则、实时发件人信誉检查、反病毒/防钓鱼保护及邮件附

件预检测、使用魔盾启发式反垃圾邮件技术的反垃圾引擎、灰色/广告邮件检测过滤、高级威胁防护、发收件人异常检测以及内容过滤分析。

为应对不断变化的邮件安全威胁，魔盾邮件安全网关内置的特征库和邮件安全策略规则将自动更新。由于邮件安全网关内的特征库和策略规则实时更新，管理员只需通过查看邮件日志的方式验证魔盾邮件安全防护的有效性即可，无需额外进行策略运维工作。当然，如果企业需要更灵活的邮件安全配置，管理员可以利用强大的策略配置功能进行自定义配置，例如：管理员可以为企业内的不同用户组/不同用户设置不同的邮件安全策略。

当邮件在连接控制模块中被判定为威胁或因某种原因被暂时拒绝连接时，邮件将被拒绝接收，而不会进行接下来的分析和投递。

当邮件在自定义策略与发件人信誉模块被判定为威胁时，邮件将被直接隔离，而不会进行之后的分析。

当邮件在自定义策略与发件人信誉模块被判定为白名单或高发件人信誉时，邮件将跳过其它分析模块，直接进入内容过滤模块进行内容过滤分析。

当邮件在此后的模块分析中被判定为威胁并进行阻挡或隔离后，将直接进入隔离区，不会进行之后的分析流程。

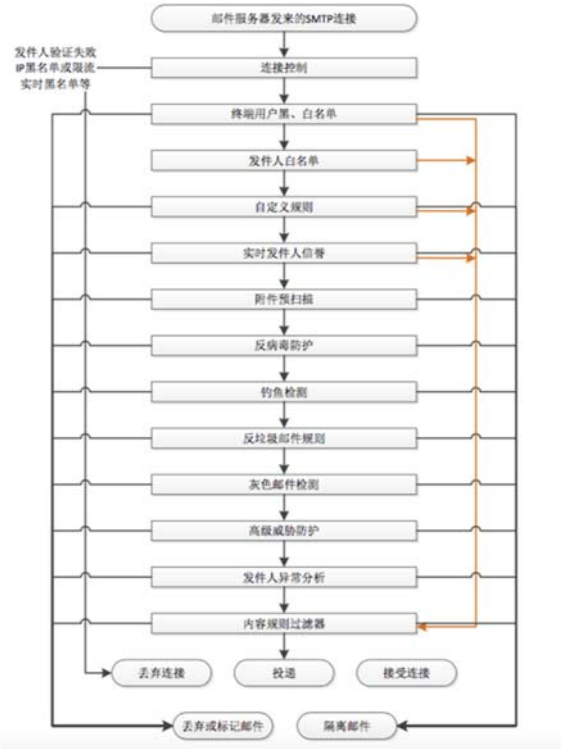

图 3-3 魔盾邮件安全网关入向分析流

对于出向邮件流，魔盾邮件安全网关按如下流程进行处理:

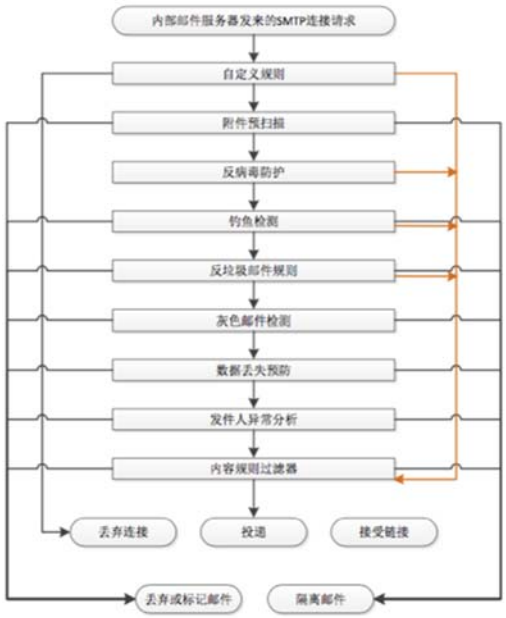

图 3-4 魔盾邮件安全网关出向分析流

四、综合威胁防御技术

魔盾邮件安全网关内置的每一层检测都提供了强大的分析能力和附加功能，而多层协同检测防御的加持可为企业提供最佳的恶意邮件防护效果。

图 4-1 魔盾邮件安全网关分析过程及动作示意图

4.1 第一层：连接控制和验证

魔盾邮件安全网关的连接控制模块支持在 SMTP 协议所在的连接层直接阻止邮件威胁并控制邮件流量，以提升邮件投递效率。连接控制模块可以实时阻断如：不符合 SMTP 协议标准的连接、超过 IP 限流或最大并发连接数的连接、发件人验证错误的连接（如 SPF 验证结果为:Fail）、低信誉发件 IP 的连接等。此外连接控制模块可以自定义设置连接 IP 黑/白名单以及开启 SMTP 服务器 TLS 验证，以确保更安全的邮件连接。

由魔盾安全综合自有网络安全数据平台与全球威胁情报源打造的发件人信誉系统，是一套强大的基于域名、IP、发件地址、收件地址、和发收件人关系等关键因子的自适应信誉数据库。通过域名/IP 大数据和网络数据关联模型分析，侦测域名、IP 和发件人在威胁活动中的行为（如：垃圾邮件、恶意软件和网络攻击等）、收件人活跃状态并对发收件人邮件行为进行学习，邮件安全网关可动态计算和生成发件人综合信誉分数，并通过信誉分数控制和过滤向客户发送邮件的发件人和邮件服务器。

在 SMTP 协议所在的连接层直接阻止邮件威胁并控制邮件流量，以提升邮件投递效率：

- 拒绝服务攻击（DoS）保护
- SMTP 连接频率控制
- 连接 IP 信誉分析
- SMTP 协议检查
- 发件人验证（SPF、DKIM、DMARC）[1]
- 发件服务器验证（TLS）

[1] SPF、DKIM 和 DMARK 是收件方借助于 DNS 记录来验证发件方真实性的重要手段。
SPF（发件人策略框架）是基于域名所有者在公网上设置的一条关于该（发件）域名的 DNS 记录，其中列出了允许发送该（发件）域名邮件的服务器 ID（公网 IP 地址）。 这使的收件方可以通过查询这条 DNS 记录来确定邮件来源的真实性。
DKIM 是 SPF 的补充，并建立了一种对域名外发的电子邮件进行数字签名的机制。通过建立协议来验证发送电子邮件的组织是否有权发送邮件，还可以防止邮件在发件人和收件人之间的传输中被篡改。
DMARK 则更进一步，除了与 SPF 或 DKIM 结合使用来实现发件人验证外，还会告知收件方服务器当 SPF 或 DKIM 检测未通过时该如何处理。

4.2 第二层：自适应发件人信誉过滤

图 4-2 发件人信誉系统分析维度

如上图所示，魔盾发件人信誉系统不止是基于静态的 IP 黑名单:

- 基于多种因素的发件人信誉分析系统，如：发件域名、连接 IP、发件地址、收件地址、发收件人关系；
- 智能与自适应，可根据用户行为自动学习和调整
- 优化的算法以保证灵活性、准确性和分析效率

图 4-3 发件人信誉分析结果

4.3 第三层：反病毒模块

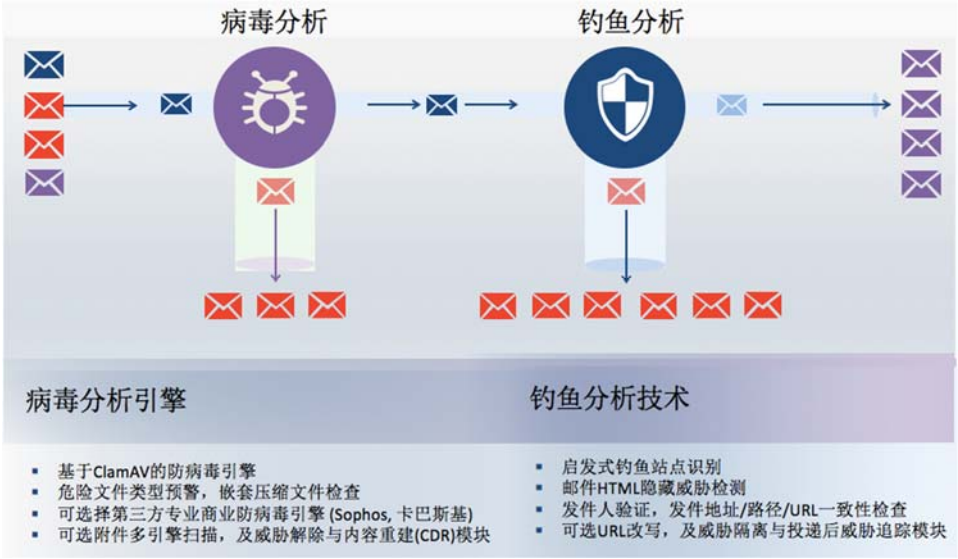

图 4-4 反病毒/钓鱼分析流

魔盾邮件安全网关配置了灵活的威胁附件检测与过滤规则，可以高效拦截可能对用户造成威胁的附件文件。魔盾邮件安全网关还内嵌了防病毒引擎，支持对病毒附件的扫描和查杀；针对客户的不同需求，魔盾邮件安全网关也支持嵌入第三方商业版本防病毒引擎作为魔盾邮件安全防御系统病毒分析的模块之一。

魔盾邮件安全网关基于 ClamAV 的防病毒引擎和/或第三方反病毒引擎以及魔盾附件预检测引擎的组合，可实现对已知威胁邮件的快速、高效识别拦截；同时对于未匹配威胁的可疑附件，可将其进行预先提取，以便下一步的分析，提升整体分析效率。

- 防病毒引擎提供全面的实时扫描和病毒库更新。 捕捉各种已知的病毒和网络钓鱼模式、间谍软件、木马、蠕虫和恶意软件威胁；

- 魔盾附件预检测引擎用于分析异常附件流量和附件文件类型，以预测和阻止潜在的附件威胁

此外，针对客户高度重视的钓鱼邮件防范需求，魔盾邮件安全网关专门开发了钓鱼分析引擎，对邮件中的钓鱼威胁进行检测和分析。通过启发式的钓鱼站点识别与钓鱼发件人/HTML/邮件内容检测，魔盾邮件安全防御系统可以高效识别可疑欺诈并对邮件进行隔离/标记操作。

图 4-5 病毒分析结果

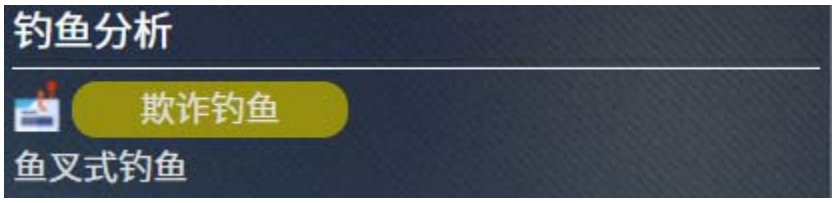

图 4-6 钓鱼分析结果

4.4 第四层：垃圾邮件/灰色/广告邮件分析模块

魔盾邮件安全网关打造的深度垃圾邮件分析引擎，通过发件人信誉与黑名单、邮件内容分析规则、机器学习规则、全球垃圾邮件投诉样本库等因素的综合分析，动态生成垃圾邮件概率，并支持用户通过垃圾邮件概率（垃圾邮件防护等级）设置邮件安全策略。

魔盾邮件安全网关预设了三种垃圾邮件判定标准，管理员可以针对企业与组织的邮件业务情况进行配置。管理员页可以自定义垃圾邮件判定阈值，对垃圾邮件判定标准进行微调。对于不同的用户与用户组，管理员可以设定不同的垃圾邮件判定阈值。

魔盾反垃圾邮件引擎可以识别并拦截 99％以上的垃圾邮件，其技术包括：

- 针对垃圾邮件的启发式内容识别规则
- 机器学习规则
- 全球垃圾邮件指纹库
- 发件人域名和 IP 黑名单
- URL 黑名单
- 其他垃圾邮件规则

灰色或广告类邮件往往处于垃圾邮件的灰色地带，用户对此类邮件的判别主观性较强。针对客户对广告订阅类邮件、商务推广类邮件的不同需求，魔盾邮件安全网关特别加入了广告邮件分析模块，帮助用户识别、分析与控制是否接收广告邮件。

广告邮件的处理方式可以设置为投递、隔离或标记。经过标记的广告邮件将在邮件标题中增加魔盾邮件安全网关添加的广告标签，便于用户针对此类邮件标题中的标签进行邮件分组或过滤。

魔盾邮件安全网关支持识别以下几类广告/商务推广邮件：

- 新闻期刊
- 推广活动
- 社交网络
- 广告

图 4-7 垃圾/广告邮件分析流

图 4-8 广告邮件分析结果

图 4-9 垃圾邮件分析结果

4.5 第五层：链接分析沙箱-钓鱼防护

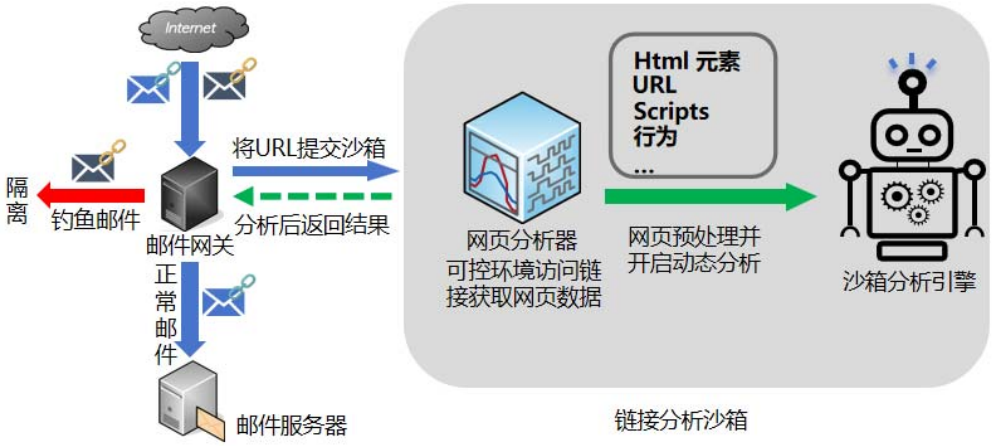

图 4-10 链接分析沙箱分析过程

魔盾链接分析沙箱作为魔盾邮件安全解决方案中钓鱼/恶意链接威胁防护的核心组件，采用轻量级沙箱技术，不仅可以通过静态匹配庞大的威胁情报库识别已知的钓鱼/恶意链接，还能针对未匹配特征的可疑链接，通过主动加载该链

接的方式获取完整的页面数据，捕捉页面代码中所有静态和动态特征，智能分析匹配钓鱼/恶意链接规则并给出威胁分数，真正做到了精准识别未知/疑似钓鱼等恶意威胁。

图 4-11、4-12 链接分析沙箱分析结果

4.6 第六层：文件分析沙箱-高级威胁防护

魔盾文件分析沙箱是魔盾邮件安全解决方案中特有的针对常规邮件反垃圾、反病毒等引擎无法识别的未知威胁/高级威胁（如：0DAY、APT、勒索软件等）的核心组件。

需要注意的是，只有当用户选择并开启高级威胁分析功能时，该功能才会生效。高级威胁分析功能开启后，邮件安全网关会将可疑邮件中的附件与链接通过 API 接口的方式传递到文件分析沙箱环境中执行分析操作。分析样本及分析结果报告的读取权限将经过文件分析沙箱严谨的隐私与安全保护措施，确保分析样本/分析结果不流入到企业网络中。

魔盾邮件安全解决方案依托强大的文件分析沙箱（ATP），邮件附件和链接传递到文件分析沙箱的分析环境中进行实时动态威胁分析。文件分析沙箱在可控虚拟环境下，模拟用户打开附件文件/链接操作，并进行一系列的静态分析及深度行为分析，生成威胁等级和威胁分析报告等。用户可以针对高级威胁的“威胁等级”设定隔离/标记等策略，对高级威胁进行过滤，最大程度的保护企业用户安全。魔盾邮件安全网关还独创的提供了互动视图威胁分析工具，帮助用户对威胁进行更深层的分析。

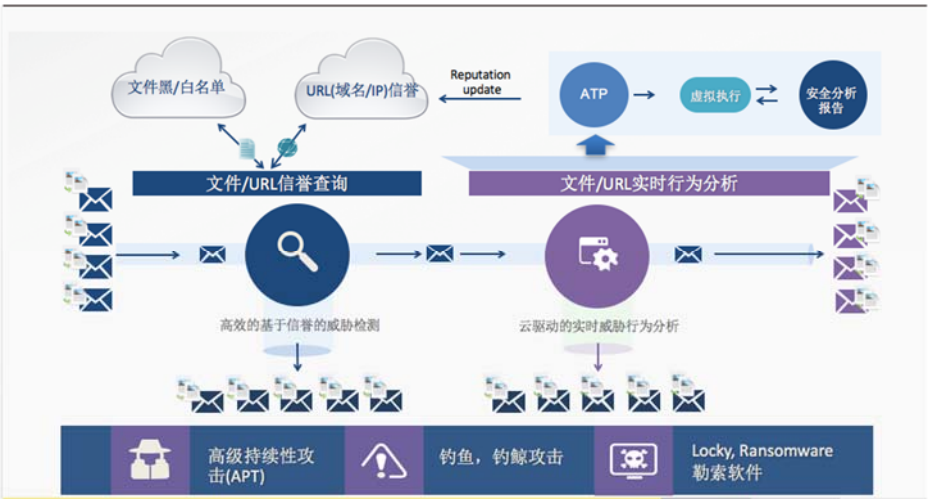

图 4-13 高级威胁分析流

魔盾邮件安全网关将邮件附件文件/URL 提交到文件分析沙箱用于防护未知威胁/高级威胁。 此时文件分析沙箱将扫描并根据结果执行下一步动作:

（1） 文件/ URL（域名/IP）信誉查询：

基于全球文件/ URL 黑名单/白名单数据库，用于快速比较和检测

（2） 动态沙盒行为分析

可疑电子邮件附件将作为加密包发送到文件分析沙箱，以进行动态行为分析

（3） 威胁云分析（可选）

魔盾邮件安全网关支持通过 API 向魔盾威胁分析云提交电子邮件附件和 URL

（4） 威胁结果输出及邮件处理

提供威胁分析结果，并可根据前期的邮件安全策略对高威胁邮件执行隔离/标记等操作

（5） 专业的分析报告

分析报告包括威胁特征、恶意文件元数据、静态分析结果、行为分析结果、网络活动和注册表摘要等。

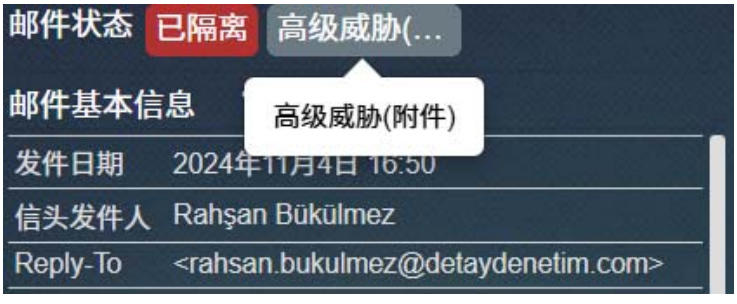

图 4-14、4-15 文件分析沙箱分析结果

4.7 第七层：异常检测

邮件流中的异常情况往往反映出邮件系统的安全状况，例如欺诈类邮件通知、伪造发件人地址或使用异常的发件人信息；而用户外发可疑邮件可能源于用户电脑系统的病毒感染。对于邮件异常的监控，往往可以帮助企业快速发现邮件中的问题并降低潜在风险。

- 发件人异常 （如：伪造、信息不符等）；
- 收件人异常 （如：密送、流量异常等）。

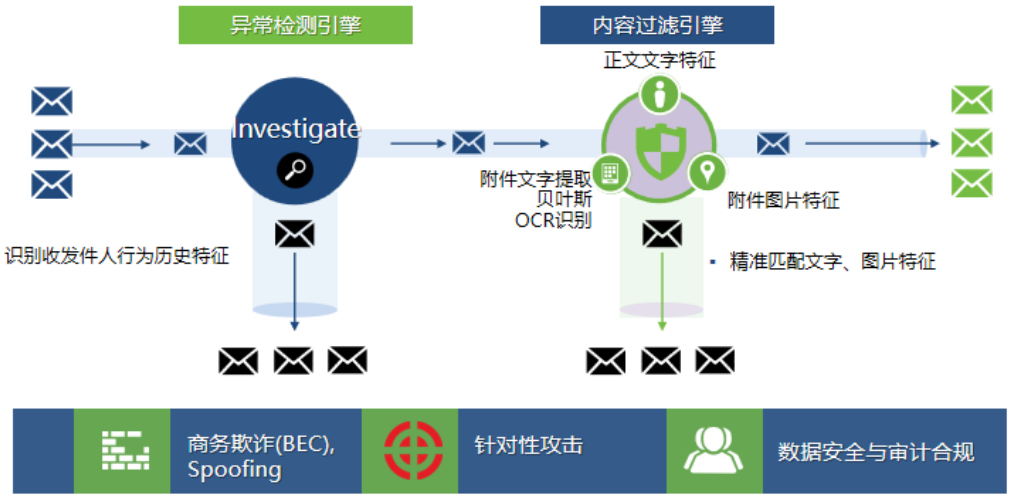

图 4-16 邮件异常分析流

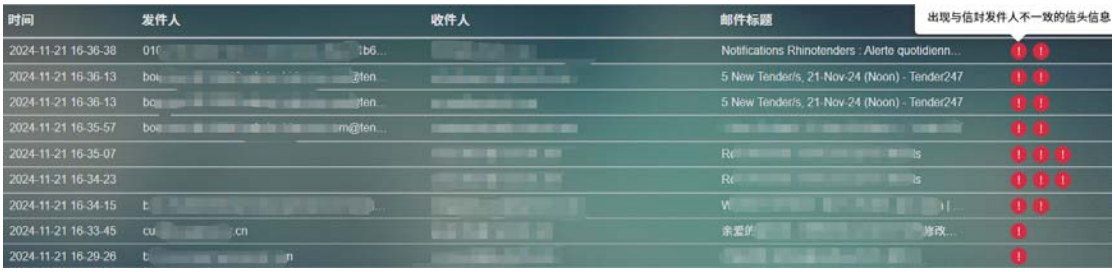

图 4-17 邮件异常分析结果

4.8 第八层：内容检测/合规

无论是出站邮件还是入站邮件，管理员都需要对邮件中的敏感信息有更加清晰的追踪能力。魔盾邮件安全网关提供额外的基于邮件内容（邮件正文、附件）的智能预定义策略与自定义策略，以实现：

- 合规分析（检查邮件正文，支持分析 OLE 格式附件、PDF 格式附件、图片附件等）
- 数据防泄漏 （预设 DLP 模版及自定义审计关键字）
- 敏感邮件处理 （如：丢弃、隔离、标记）
- 自定义处理 （如：通知发件人、通知收件人、通知特定邮件地址等）

五、分析追踪与人工智能

除了全面的邮件威胁分析防护技术，魔盾邮件安全解决方案还创新的提供了分析追踪工具与人工智能助手。

分析追踪工具支持邮件管理员和安全管理员对企业的邮件进行分析，对威胁进行追踪。支持的功能包括

- **发件人分析：**查询与分析发件人信息，包含信封发件人、信头发件人名称、信头发件人地址、回复地址、及发件人异常情况等。
- **收件人分析：**查询与分析收件人信息，包含信封收件人、信头收件人地址、抄送地址、及收件人异常情况等。

- **附件追踪：**查询与分析邮件中的附件信息，包含文件名、MD5 哈希、状态、流量情况等。
- **URL 追踪：**查询与分析邮件中的链接，包含域名、URL、状态等。
- **发件人验证：**查询与分析邮件发件域名、连接 IP 以及发件人验证情况，包含 SPF、 DKIM、 DMARC。
- **发收件人关系：**查询与分析发件人与收件人的邮件往来、邮件状态、异常情况等。

图 5-1 分析追踪功能矩阵

魔盾邮件安全人工智能助手是基于人工智能、针对企业邮箱用户的个人邮件辅助工具。AI 助手可以学习用户的邮件处理行为，预测用户的邮件接收偏好，自动帮助用户调整邮件安全设置。

六、策略管理

6.1 管理界面

魔盾邮件安全网关提供了一个可视化的策略管理界面，允许管理员完全控制修改现有邮件安全策略，轻松配置或调整邮件的防护功能。

图 6-1 魔盾邮件安全管理界面

邮件安全网关的管理员需要随时掌控邮件流的情况。魔盾邮件安全网关通过一套丰富的图表报告和仪表盘系统提供可视化的邮件流量和邮件类型信息。

图 6-2 魔盾邮件安全网关主页威胁视图

魔盾邮件安全网关的策略和管理功能包括但不限于

6.2 管理功能

- **Web UI 管理界面：**支持中文/英文的 Web UI 管理界面；
- **CLI 管理接口：**支持 CLI 命令行接口管理；
- **远程技术支持：**支持远程技术协助功能；
- **分域用户管理：**支持多管理员账号设置，可为不同邮箱域名指定不同管理员，可针对不同邮箱域名设置完全不同的邮件安全策略；
- **分用户/用户组管理：**支持针对不同的用户或用户组，设置完全不同的邮件处理策略；
- **SYSLOG：**支持对接单个/多个 SYSLOG 服务并输出 SYSLOG 日志。协议层面支持 UDP/TCP 协议；

- **SNMP：**支持 SNMP 系统状态监控；支持多个 trap 地址设置；支持 SNMP V2 及 V3；
- **LDAP 同步：**支持与企业 LDAP 服务器进行对接；
- **分用户设置黑名单：**支持用户自定义黑名单与白名单，不与全局策略相冲突；
- **分用户邮件策略：**支持为不同用户设置不同的邮件安全策略；
- **分用户邮件管理界面：**支持用户登录 Web 界面查阅自己的邮件日志、设置黑白名单等；
- **人工智能学习：** 人工智能与自适应机器学习加持下，预测用户邮件偏好，自动帮助用户调整策略。

6.3 防护功能

- **邮件防火墙：**有效防护针对邮件通讯协议 SMTP 的攻击，以此保证邮件服务器不被黑客攻击，保持高性能与高稳定性；支持在 SMTP 连接层进行流量控制；有效防止 Open Relay（开放转发或匿名转发），只接收用户目标域名邮件，防止邮件网关被利用并传递垃圾邮件；
- **垃圾邮件特征与情报更新：**垃圾邮件特征与情报云端实时更新，每 10 分钟更新一次，达到实时防护效果；
- **垃圾邮件特征优化：**支持人工智能自动根据用户行为（误判、漏判、释放、添加黑白名单）对该用户的垃圾邮件评分标准进行动态调整；

- **DKIM：** 支持 DKIM 协议的发件人身份验证。
- **DMARC：**支持 DMARC 协议的发件人身份验证。
- **病毒查杀引擎：** 内置的防病毒功能，支持统一管理病毒邮件过滤；防病毒模块可根据用户需求，支持单独配置启用或禁止，不影响正常垃圾邮件过滤功能。
- **病毒爆发保护：** 支持威胁附件预警，可以在不依赖病毒特征库的情况下对可疑恶意软件爆发进行监控和隔离。

6.4 反垃圾邮件引擎

- **基于规则的评分：**基于启发式垃圾邮件规则的评分系统；
- **内容过滤：**具有启发式过滤技术，能够识别未知类型的垃圾邮件。启发式过滤技术敏感等级可根据企业邮件业务情况进行自定义；
- **邮件头过滤：**支持根据邮件头数据进行分析判断；
- **机器学习技术：**具有基于本地数据的邮件机器学习与垃圾邮件判定功能；
- **邮件处理日志：**具有邮件日志跟踪功能，能够监控每一封邮件接收、处理、发送情况，保证邮件的正常发送与接收；
- **分析引擎：**内容识别、机器学习、信誉数据分析、模糊哈希指纹技术等多种分析引擎加持；
- **图片识别技术：**支持正文、附件内的图片内容识别能力；

- **指纹分析技术：**具有针对邮件内容的指纹分析计算能力；
- **发件人特征识别系统：**检查发件人域名是否符合标准协议，支持对发件人地址执行 DNS 查询并基于查询结果进行处理；
- **发件人欺骗保护功能：**支持自定义策略、发送者策略框架 (SPF)及发件人异常检查；
- **收件人特征识别系统：**支持通过收件人邮件状态与邮件处理行为，智能判断收件人偏好与邮件处理方式；
- **发收件人关系识别：**支持通过发收件人邮件往来历史，智能判断针对不同收件人的发件人信誉；
- **广告/灰色邮件分析：**支持针对广告邮件、灰色邮件的特殊分类分析；
- **多条件自定义规则：**支持高度自定义规则过滤功能，通过自定义过滤规则或多条件规则组合，可阻止符合某些特定的附件类型、文本内容、主题、发收件人信息以及符合其他标准的邮件；
- **全球信誉系统：**具备发件人信誉评价体系，对发件域名、连接 IP、 发件人地址、收件人地址、发收件人关系等多重因素进行实时信誉与历史行为评分，动态调整与自适应，不止是黑白名单；
- **多语种邮件分析支持：**支持对基于不同语言的邮件过滤能力，专注于中文、英文、俄文、日文以及韩文等高发语种。

6.5 高级功能

- **高级/未知威胁保护：**文件分析沙箱可与邮件网关无缝结合，结合静态特征分析与沙箱动态行为分析，可防护邮件内的高级/未知威胁；
- **SMTP TLS 加密协议：**支持 SMTP+TLS 加密协议；
- **邮件负载均衡：**支持根据不同邮件地址进行不同邮件路由的功能，并支持多重路由；
- **静态路由策略：**支持静态路由策略；
- **管理员高级故障诊断：**支持管理员高级故障诊断；
- **邮件加密功能：**支持基于 AES-128 的邮件加密，可以通过自定义规则和内容过滤策略触发；
- **针对 BEC 高管欺诈的 VIP 邮箱设置：**支持 BEC 邮件欺诈防御功能；
- **蜜罐邮箱：**支持蜜罐邮箱以收集特定垃圾邮件信息；
- **支持统计报告：**支持多种针对邮件流量、邮件特征和邮件状态的图表报告，以饼状、线性、柱状图表等形式提供；
- **报告格式：**支持 HTML、CSV、PDF 格式导出；
- **实时报告图表：**支持实时提供各种报表明细统计；支持自制与自定义各式报表；
- **高级威胁报告：**支持高级威胁报告订阅、接收高级威胁警报；

- **行政汇报报告：**支持丰富的管理层报告，帮助管理人员理解邮件流状态与邮件安全趋势；
- **分析追踪功能：**支持针对发件人、收件人、附件与邮件链接的搜索、分析和追踪功能；
- **邮件日志处理：**支持邮件分析功能，除了针对邮件处理的所有记录与威胁判定原因分析，还可针对各项参数进行深度分析；支持邮件日志历史记录查询与威胁情报查询。
- **外发邮件控制：**支持外发邮件策略配置在一个平台上完成；
- **自定义邮件路由：**支持根据自定义策略（如发/收件人等）触发邮件路由策略；
- **合规与数据防泄漏：**支持通过内置内容过滤与 DLP 功能进行敏感信息与数据检查，对不合规邮件进行隔离审查；
- **异常行为分析：**支持预设异常行为规则，可针对发收件人的异常行为进行监控和隔离；
- **附件文字与图像处理：**支持针对文档（OLE）附件的文字提取；针对图片附件，同时支持 OCR 图像文字识别与 CV 图像特征分析；针对 PDF 附件，支持同时进行文字提取分析与图像分析；
- **隔离邮件报告与用户释放：**支持用户隔离邮件管理，用户可以自定义垃圾邮件隔离报告发送时间，支持一日多次自行设定；

- **自动告警与报告订阅：** 支持系统出错及系统故障时提供基于报告订阅的自动告警功能。

6.6 归档功能

- **邮件检索 ：**提供方便快捷的邮件搜索入口，包含常用的查询方式，如：关键词（提供高级搜索功能）、邮件主题、发件人与发件域名、收件人与收件人域名、附件类型、时间与日期、标签与注释等多种维度；

- **分权管理：**可整合企业组织架构，按部门、群组或者用户身份进行邮件的检索和查询；另可设定部门主管仅审计查看自己所管辖的部门内用户的归档邮件，实现分权管理 。每个用户也支持个人归档邮件管理功能，在管理员设定的权限范围内， 每个用户可以自主登录归档系统，对自己个人的历史邮件进行搜索、下载、批量导出等操作；

- **高速搜索：**通过 Sphinx 索引技术，可轻松应对在企业历史归档数据不断增长的情况下，依然保持优秀的邮件搜索效率。

6.7 高可用性与扩展功能

- **高可用功能：**邮件安全网关支持高可用部署方式，支持对下一跳邮件地址进行负载均衡设置；

- **灵活的部署形式：**邮件安全网关、文件分析沙箱及链接分析沙箱产品均支持软硬件一体（Intel X86/国产化 X86 架构）、纯软件部署（虚拟

化/私有云部署，支持 VMWare ESXi/vSphere、KVM 等多种虚拟化部署）、云托管部署等多种部署形态；产品组合上，支持纯网关模式（仅邮件安全网关）、纯沙箱模式（仅文件安全沙箱、链接分析沙箱）、特定类型增强分析模式（邮件安全网关+文件/链接分析沙箱）及全威胁防御模式（邮件安全网关+文件分析沙箱+链接分析沙箱）；部署架构上，支持网关模式（部署在企业邮件业务出口）、串联模式（部署在企业现有邮件网关及邮件系统间）及旁路模式（部署在企业邮件业务侧）。集群部署环境下，支持双活（主主）模式及主备模式；

- **API 接口扩展：**产品内置 API 接口，支持第三方设备通过 API 或 SMTP 形式对邮件进行扩展分析。

6.8 安全功能

- **底层操作系统：**基于 Ubuntu 系统采取安全加固并高度定制；同时也支持在国产化操作系统下进行部署；
- **外发威胁速率控制：**监控内部用户有无因盗号等因素导致外发恶意邮件的情况。通过对企业邮箱配置账号速率控制，可避免内部账号因被密码被暴力破解后充当跳板大量外发、滥发垃圾/恶意邮件，而导致企业网络地址被列 RBL，影响企业邮件业务的正常运行；
- **管理员权限：** 支持可以针对邮件域名设置多个管理员，并分配不同的管理权限；

- **安全审计：**支持用户操作记录日志的查看；
- **登录管理：**支持管理员用户安全策略功能，如密码锁定次数、密码复杂度、用户有效期、用户登录时间限制等。

七、部署方案

从部署角度来看，魔盾邮件安全网关支持多种部署方式：支持软硬件一体（Intel X86/国产化 X86 架构）、纯软件部署（虚拟化/私有云部署，支持 VMWare ESXi/vSphere、KVM 等多种虚拟化部署）、云托管部署等多种部署形态；产品组合上，支持纯网关模式（仅邮件安全网关）、纯沙箱模式（仅文件安全沙箱、链接分析沙箱）、特定类型增强分析模式（邮件安全网关+文件/链接分析沙箱）及全威胁防御模式（邮件安全网关+文件分析沙箱+链接分析沙箱）；部署架构上，支持网关模式（部署在企业邮件业务出口）、串联模式（部署在企业现有邮件网关及邮件系统间）及旁路模式（部署在企业邮件业务侧）。

7.1 工作流

魔盾邮件安全网关可以在企业网络中被设置为负责接受外域邮件的邮件网关。从外域发往用户邮箱域名的邮件，根据域名 MX 记录的指向，先经过魔盾邮件安全网关，通过邮件安全网关的邮件分析与过滤后，再投递到企业内部邮件服务器。

（注： 由于魔盾邮件安全解决方案包含连接控制与验证、反垃圾邮件、反病毒、高级威胁分析等功能模块，并集成了强大的邮件威胁信息与分析能力，我

们建议企业将魔盾邮件安全网关作为入向邮件过滤分析的入口，或邮件安全分析的第一步。如果已经部署了邮件防病毒（AV）/反垃圾邮件（AS） 等邮件安全产品，企业可以将魔盾邮件安全网关部署在其它邮件安全系统之前以获得最优的过滤分析效果。根据企业需求，魔盾邮件安全网关也可以部署在用户网络中其它邮件安全产品之后。）

如果邮件被魔盾邮件安全网关判定为垃圾邮件或高级威胁等，并且用户策略设定为隔离的，邮件将被邮件安全网关存入邮件隔离区，而不会继续投递。用户可以通过邮件安全网关的管理平台或隔离邮件报告对邮件安全网关隔离区中的邮件进行释放。释放后的邮件将从邮件安全网关投递到企业内部邮件服务器。

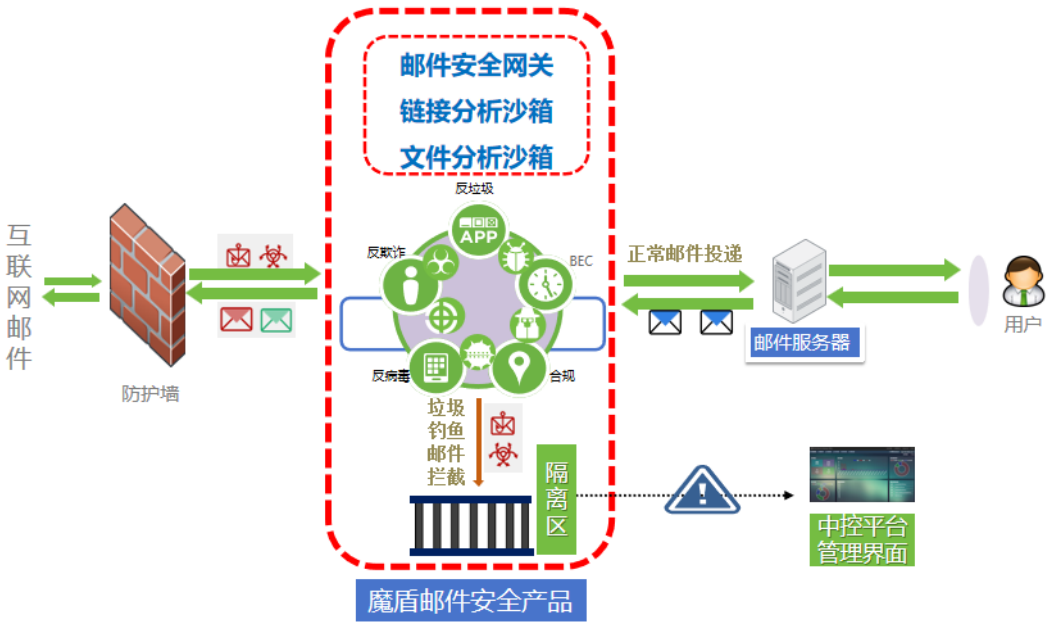

图 7-1 魔盾邮件安全产品部署架构

7.2 部署架构

对于存在多节点部署、单一节点内需部署多台邮件安全等较大的网络环境，管理员可以通过部署一台或多台集群中控平台以管理其邮件安全网关设备，轻松

扩展魔盾邮件安全部署。 在这种情况下，邮件安全网关设备用作网关 MTA，处理入站/出站邮件并将分析后的邮件转发到其他邮件服务器。

对于托管邮件服务器，或需要云端部署的企业，魔盾邮件安全解决方案支持云交付的邮件安全服务，用户可以设置邮件域名的 MX 纪录使邮件先进入魔盾邮件安全云服务， 经过分析过滤后，再传递到用户邮件托管服务器。

魔盾邮件安全网关也可以在用户网络中同时被设置为负责接受内域邮件的邮件网关。从内域用户邮箱发出的邮件，由用户邮件服务器投递至魔盾邮件安全网关，通过邮件安全网关的邮件分析与过滤后，再对外投递到最终收件地址。

入站邮件：

邮件由互联网进入魔盾邮件安全网关，经过魔盾邮件安全网关或云产品分析处理后，邮件将根据域名或者收件人的策略投递到响应的邮件服务器。

出站邮件：

邮件由用户指定的邮件服务器进入魔盾邮件安全网关，经过魔盾邮件安全网关或云产品分析处理后，邮件将被传递给收件人邮件服务器。

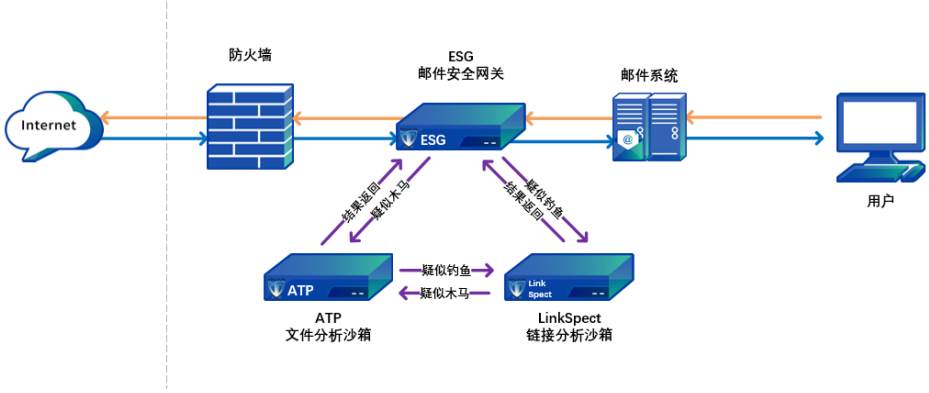

图 7-2 魔盾邮件安全解决方案标准部署拓扑图

八、产品亮点总结

8.1 轻松管理

- **部署灵活：**可选择软硬件一体、纯软件（虚拟化）、云托管或混合部署的邮件安全网关，适用更多场景；定制化产品形态可保证最优的邮件处理性能；
- **维护简单：**快速高效的网关接入配置与系统规则更新；高度智能的管理界面、灵活的策略与规则设置、全面的邮件流控制；
- **人工智能：**人工智能助手学习用户行为，预测用户偏好，自动调整用户策略；减轻管理员负担，增加管理效率。

8.2 全面防御

- **智能信誉：**基于发件人信息与发/收件人关系的智能自学习发件人信誉系统，通过发件人综合信誉高效提前阻截邮件威胁；
- **全面扫描：**利用多层邮件分析技术对邮件内容、模式、指纹等信息进行深度扫描，可独立控制的广告邮件与钓鱼邮件分析模块；
- **高级威胁：** 结合静态分析与动态沙箱扫描，对邮件附件与链接进行触发式实时深度分析，防御未知威胁，生成高级威胁报告；

8.3 技术支持

- **尖端技术 ：**异常检测、内容过滤、附件文本与图像识别、邮件大数据分析与威胁特征机器学习；
- **技术支持：**多年邮件安全产品经验的顶尖安全团队自主研发，邮件安全专家随时待命为您解决任何问题。

8.4 工具创新

- **分析工具：**独创的引入了 Investigate（分析）功能与高级威胁视图分析工具，让管理员与安全团队更高效的掌控威胁因素，追踪威胁轨迹；
- **威胁情报：**威胁情报的集成与威胁信息的展示，将魔盾邮件安全解决方案转化为邮件威胁分析与数据提取的平台。

8.5 结论

企业邮件流量中超过一半被垃圾邮件、恶意邮件等占据，极大程度地影响了企业及员工的业务效率。其中，垃圾邮件、恶意邮件又往往是向企业发起攻击的重要手段，邮件内附件文件、图片、URL 链接等是最常见的邮件攻击方式。企业需要通过各种方式，对邮件业务进行防护，有效保护核心业务、资产及数据、降低潜在风险。魔盾邮件安全解决方案综合了高效、多维度的发件人信誉系统、强大的垃圾邮件内容深度过滤系统、独立的病毒分析、钓鱼邮件分析、广告邮件分析，以及专业的高级威胁分析（附件/URL），一站式阻截基于邮件的各种安全威胁：

高效的威胁防御：全面的防御技术，一站式阻截通过邮件传递的威胁；高效病毒分析与附件预检测，阻挡附件中隐藏的已知威胁；强大的垃圾邮件分析技术，多种算法计算垃圾邮件概率；同时独立检测钓鱼邮件与灰色（广告）邮件； 动态威胁行为分析，拦截高级未知威胁，如高级针对性威胁(APT)、勒索软件等； 基于智能发件人信誉与异常检测，有效侦测商务邮件欺诈(BEC)、欺骗(Spoofing)及其它异常； 内容过滤与合规分析，搜寻敏感信息，灵活处理违规邮件。

灵活和高性价比：结合企业与组织网络架构，可选择软硬件一体、纯软件（虚拟化）、云托管或混合部署的邮件安全网关； 定制化产品形态与功能开发，保证最优化的威胁检测能力和最严格的邮件处理要求 ； 强大的邮件流控制功能及灵活的策略与配置，适应不同场景与需求； 人工智能助手，自适应与自学习，降低维护与管理成本，减轻管理员负担； 丰富的数据，报表与独特的分析功能，帮助企业精准了解邮件威胁，为企业安全人员提供高效的分析工具及报告。

尖端技术与创新：魔盾核心技术团队具有超 20 年的邮件安全行业经验，具备顶尖的邮件威胁分析能力，确保邮件威胁趋势与最新垃圾邮件检测技术有效应用在邮件安全网关及其他邮件安全产品中； 自研下一代的邮件安全引擎，基于信誉、内容、行为分析的高效整合，实时快速识别未知威胁； 顶尖的自动化恶意软件分析能力支撑，可提供专业威胁分析报告； 自适应机器学习的应用，嵌入人工智能助手，建立与企业用户的互动； 独特的分析(Investigate)功能，以威胁情报，关系模型和智能工具辅助威胁追踪与安全防护。