请扫描二维码
获取更多安全资料

勒索软件防御验证设计指南

SAFE 设计指南

安全领域：威胁防御

2016 年 9 月

2017 年 2 月 10 日更新

SAFE
SIMPLIFIES SECURITY

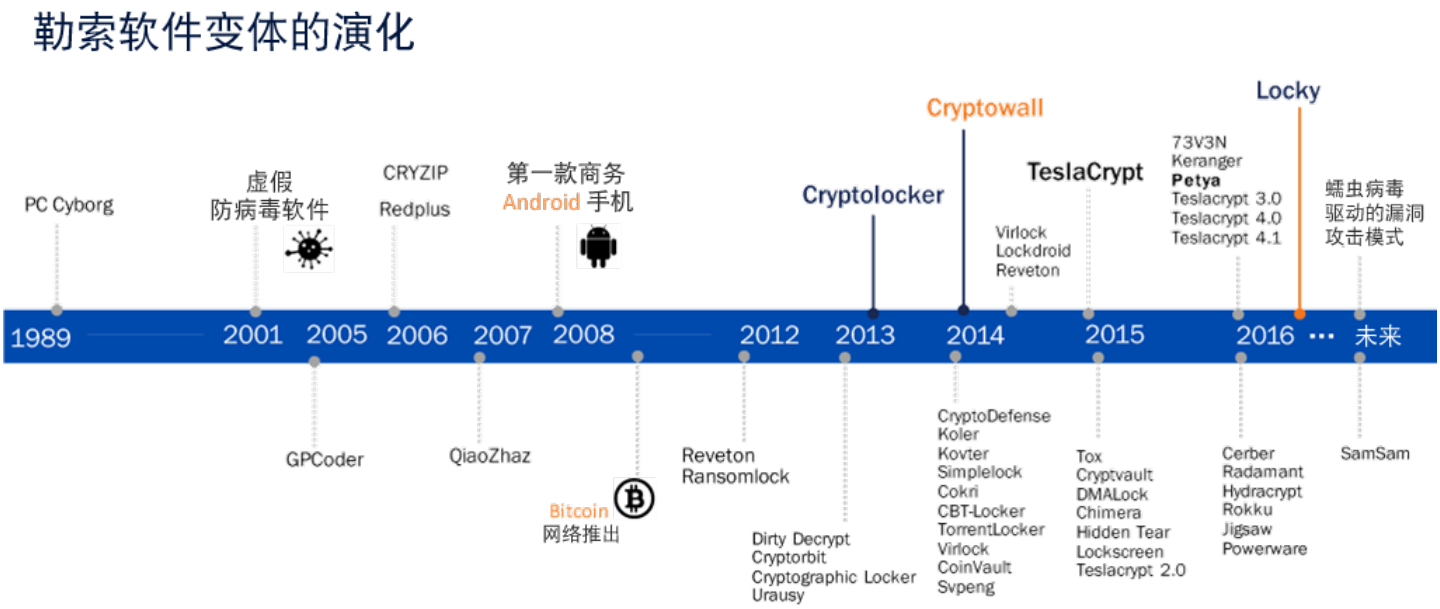
目录

简介

勒索软件是有史以来获利最丰厚的恶意软件类型。过去，恶意软件通常不会导致系统拒绝访问，也不会破坏数据。攻击者的主要目的是窃取信息，并保持对受害者的系统和资源具有长期访问权限。勒索软件改变这个惯例，从不易察觉地暗中访问变成明目张胆地敲诈勒索。

支付赎金恢复文件的每一家企业或每一个人，都是直接向攻击者进行付款。匿名货币（例如比特币和瑞波币）这种相对新鲜的新生事物为攻击者提供了以相对较低的风险轻松牟利的途径，让勒索软件得以创造暴利并为开发下一代勒索软件提供资金。因此，勒索软件正在以惊人的速度演化（如图 1 所示）。预计未来的版本将像蠕虫一样传播，以经过协调的方式在整个组织中扩散，并要求一笔总赎金。

图 1 - 勒索软件的演化



2016 年前 3 个月，网络犯罪分子通过解锁计算机敲诈企业和机构，所获得的非法所得达到 2.09 亿美元。按照这种情形，勒索软件今年将成为每年牟利高达 10 亿美元的犯罪产业。
仅今年一年，Angler 漏洞攻击包（它会感染系统并部署勒索软件）就攫取了 6000 多万美元非法收入 [1]。

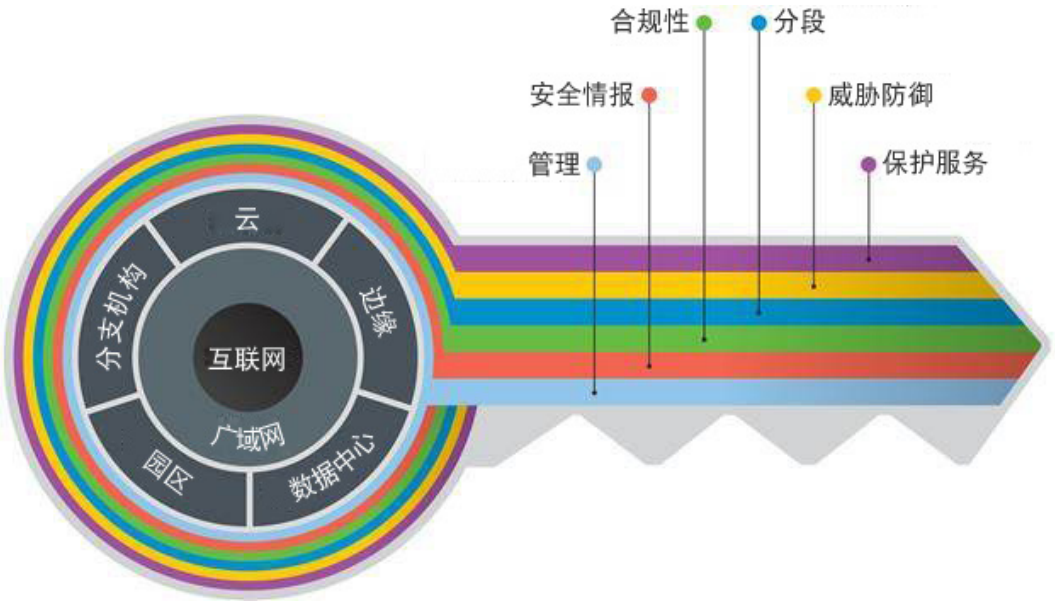
思科可以使用深度防御架构帮助企业防御勒索软件威胁，在网络内外保护企业用户的安全。

[1] 勒索软件：过去、现在和未来 - http://blog.talosintel.com/2016/04/ransomware.html

SAFE 简介

SAFE 通过实施一种特有的模式，重点关注组织必须保护的方面，从而简化整个企业的复杂性。如图 2 所示，此模式将各个安全领域作为一个整体来对待，侧重点是当今的威胁，以及各个安全领域防御这些威胁所需具备的功能。思科已对这些重要业务挑战进行部署、测试和验证。

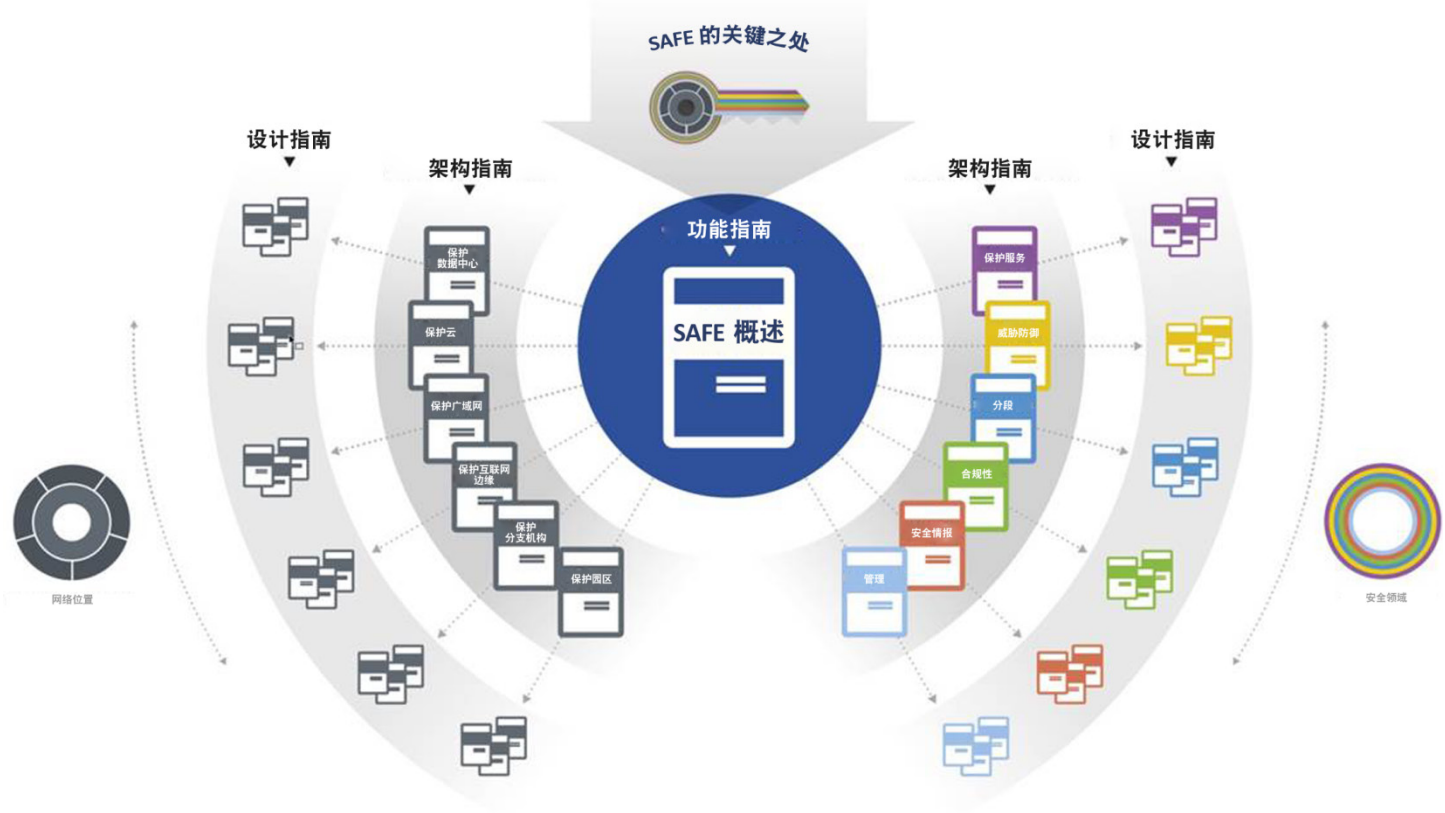
图 2 - SAFE 解决方案



SAFE 的关键之处在于将整体安全解决方案的复杂性分解到各个网络位置 (PIN) 和安全领域中。

如图 3 所示，SAFE 从复杂性角度出发，根据受众需求来简化端到端安全。从各种业务流及其伴随的威胁，到相应的安全功能、架构和设计，SAFE 可以提供清晰易懂的全面指导。

图 3 - SAFE 指导



有关思科 SAFE 如何简化安全解决方案的更多信息，请访问：www.cisco.com/go/safe

本设计指南介绍 SAFE 威胁防御领域下的勒索软件具体使用案例。本解决方案使用案例的设计验证包括云服务和云产品。此外，本指南还包括推荐的园区 PIN 架构（仍在进行验证测试）。

勒索软件概述

有些恶意软件可能会锁定公司和个人的关键资源以进行要挟，这种恶意软件称为勒索软件。勒索软件使用传统恶意软件攻击媒介（例如网络钓鱼邮件和漏洞攻击包）来向桌面传输勒索软件。攻击成功后，勒索软件可以控制系统和存储的数据，加密其中内容，使其拒绝访问，以此进行要挟，直到获得赎金。勒索软件使用完善的公钥/私钥加密方法，使得人们仅可通过支付赎金或从备份中恢复这两种方案重获文件。攻击者通常会在勒赎要求获得满足后提供用于恢复访问的解密密钥，但也未必一定会这么做。

拒绝对这些重要资源进行访问可能会给企业带来灾难性的后果：

- 医疗业 - 医院可能会丧失即时为患者提供护理的能力（收治入院、手术，药物治疗等）
- 公共安全 - 应急人员可能无法响应报警电话或紧急呼叫
- 金融业 - 银行系统的交易活动或银行业务活动可能会脱机
- 零售业 - 无法处理付款，致使顾客无法购物

勒索软件感染

图 4 - 典型的勒索软件感染步骤

1. 勒索软件一般通过大规模的网络钓鱼活动、恶意广告或针对性的漏洞攻击包投放。
2. 待投放到系统中后，勒索软件会控制您的系统，并试图与其命令和控制基础设施通信，以便创建和传输用于加密文件的公钥/私钥。
3. 勒索软件获得必要的密钥后，会确定要加密的特定文件类型和目录，并避开各种系统和程序目录，确保在其结束运行后能够稳定地交付赎金。
4. 加密完毕后，勒索软件会给用户留下通知，说明如何支付赎金。

组织中的常见感染媒介

组织可能因多种方式而受到勒索软件入侵。最常见的方式包括邮件网络钓鱼攻击和网络中挂载的恶意广告。

> 邮件 - 在使用了分发列表和大规模邮件群发的情况下，邮件是一对多感染媒介。通常情况下，一名用户会拥有多个邮件帐户，既有个人帐户也有公司帐户。每个帐户都意味着一个安全威胁。例如，尽管 IT 部门会付出大量时间和精力选择邮件安全服务（例如思科邮件安全设备或云），但用户使用 Hotmail 和 Gmail 等公共邮件服务查收个人邮件的情况却屡见不鲜。通过 Web 门户可以轻而易举地绕过这些邮件安全服务访问此类私人邮件帐户。从这些帐户访问、下载并执行邮件附件和网络钓鱼链接是一个重要的安全隐患。

网络 - 恶意广告是犯罪分子控制的广告，它会蓄意感染系统，直接安装漏洞攻击包或勒索软件。恶意广告可能是任何站点上的任何广告，而且这些站点通常是我们每天都要访问的站点。当用户点击广告时，便会跳转到某个站点，导致其计算机受到感染。恶意广告网络包括数千个网络域名，这构成了一个不断变化的共享基础设施。这些域名可能是随机或半结构化的域名，但共同特征是寿命都相对较短，而且经常更换。这些域托管着犯罪分子用于感染、控制和中断系统的漏洞攻击包、工具以及命令和控制服务。这些通信几乎全部都经过加密。

用户可能因多种方式而碰上恶意广告，例如只是访问了推送广告的网站或者点击了搜索结果页面或邮件中的链接 [2]。经验丰富的网民通常会在系统上实施广告拦截器来获得保护，但这会影响站点的广告收入，因此目前关于限制内容和要求禁用广告拦截器存在很大争议。虽然各大站点可以根据广告拦截器的使用限制对其网站的访问，但这些发布者无法保证其推送的广告不是恶意广告。这些站点和服务是入侵和重新定向的主要目标。

勒索软件的演化和发展来势汹汹。它们吸收其他恶意软件（例如尼姆达、震荡波蠕虫、红色代码、SQL 蠕虫王、Sality，飞客蠕虫）最有攻击性的功能，在整个企业网络中扩散和感染，加密其可以访问的所有数据，力图索取总额更大的赎金。为了对这种未来趋势做好准备，具有深入网络可视性的深度防御架构将对网络的防护发挥重要作用。

[2] http://blog.talosintel.com/2016/05/spin-to-win-malware.html

勒索软件的通信

如表 1 所示，勒索软件的通信包括用于获得加密密钥和付款消息的命令和控制 (C2) 回调方法。

表 1 - 勒索软件的通信方法

	加密密钥				付款消息
名称*	**DNS**	**IP**	**无 C2**	**TOR**	**付款**
Locky	✓	✓			DNS
SamSam			✓		DNS (TOR)
TeslaCrypt	✓				DNS
CryptoWall	✓				DNS
TorrentLocker	✓				DNS
PadCrypt	✓				DNS (TOR)
CTB-Locker	✓			✓	DNS
FAKEBEN	✓				DNS (TOR)
PayCrypt	✓				DNS
KeyRanger	✓			✓	DNS

* 截至 2016 年 3 月最主要的变体

成功侵入系统后，漏洞攻击包会分析所处环境（例如操作系统、未打补丁的应用等），继而检索并投放有效的勒索软件变体。然后，漏洞攻击包会向勒索软件基础设施发出回调通信，检索加密系统所需的密钥。许多最常见的漏洞攻击包和勒索软件变体会将域名解析为 IP 地址来启动此回调。

虽然有些勒索软件变体的表现不同（例如 SamSam 使用不需要 C2 回调的内置加密密钥，而其他变体使用基于 Tor 的洋葱路由或无需 DNS 的纯 IP 回调），但勒索软件防御解决方案仍可通过许多方式发挥作用。

勒索软件杀伤链

如图 5 所示，上文概述的感染过程的前两步通常划分为七个攻击阶段。并非所有攻击都会用到每个阶段，但这些是最常见的阶段。

图 5 - 攻击的七个阶段

术语“杀伤链”指部署正确应对措施时，在以下任何特定阶段拦截攻击的能力。下面对这些阶段进行了简要描述。它们在安全行业内广为人知，但名称可能略有出入 [3]。

侦测： 攻击者收集有助于创建看似可信的站点和邮件的信息，以便掩饰恶意广告和网络钓鱼邮件。

准备： 网络犯罪分子使用在侦测阶段收集的信息尝试诓骗用户打开邮件或点击链接。

启动： 传输站点从看似可信的站点重新定向至用于启动漏洞攻击包和/或打开其他恶意内容的站点。

利用： 用户进入被入侵的站点时，攻击者将扫描其系统是否存在漏洞，进而利用相关漏洞控制用户的系统。

安装： 成功利用漏洞获得控制权后，攻击者将在目标上安装感染和加密受害者计算机的最终投放文件/工具，即勒索软件负载。攻击者还可能在该阶段额外安装可执行文件，以便在未来传输其他恶意软件。

回调： 一旦感染，恶意软件将“回调”命令和控制服务器 (C2)，在其中检索用于执行加密的密钥或接收其他指令。

持续： 攻击者将硬盘、映射的网络驱动器以及 USB 设备上的文件加密，并发出通知或部署启动屏幕弹窗，说明如何支付赎金以恢复原始文件。该通知会持续存在，有时还会删除文件，同时显示倒计时器，指示获取解锁密钥的可用时间，给用户带来巨大压力。此外，漏洞攻击包可能持续存在并转移至其他更关键的系统。

[3] http://www.cisco.com/c/en/us/products/security/annual_security_report.html

勒索软件防御

勒索软件防御解决方案使用思科安全最佳实践、产品和服务创建深度防御架构，用于防止、检测和响应勒索软件攻击。

思科的勒索软件防御解决方案并非灵丹妙药或万全之策，但确实有助于：

- 尽可能防止勒索软件进入企业
- 在系统级别阻止勒索软件，不让其获取命令和控制权限
- 检测网络中存在的勒索软件
- 尽量遏制勒索软件扩散到其他系统和网络区域
- 执行事件响应，修复漏洞和受到攻击的区域

此解决方案可以帮助保持运营的正常运转，减少对受到要挟和丧失关键系统控制权的担心。

为了防御勒索软件杀伤链，需要以特定功能打造相应的防御层。表 2 列出了 SAFE 方法中最适合此防御的功能（以蓝色图标代表）。

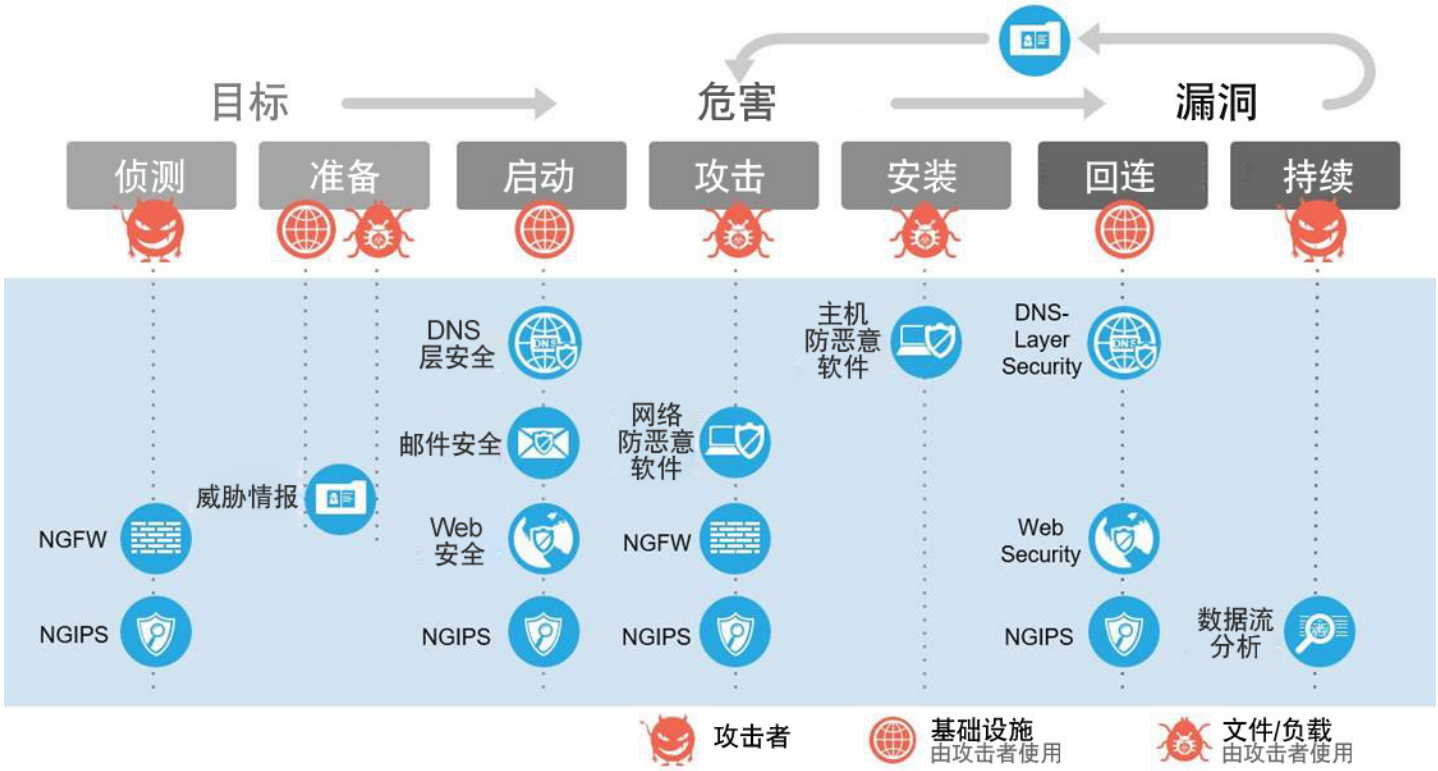
表 2 - 用于防御勒索软件攻击的 SAFE 功能

图标	功能	作用
	威胁情报	了解现有勒索软件和通信媒介，并学习新威胁的相关知识
	邮件安全	拦截勒索软件附件和链接
	DNS 安全	拦截已知恶意域名，并断开 C2 回调
	客户端安全	检查文件中是否存在勒索软件和病毒，并视情况进行隔离和清除
	Web 安全	拦截指向已感染站点和文件的 Web 通信
	基于身份进行防火墙分段	基于角色和策略实施访问验证和流量分离

	入侵防御	拦截攻击、漏洞利用和情报收集活动
	网络监控	使用基于流的分析监控基础设施通信；识别异常流量并发出警报

如图 6 所示，随后将部署上述每项功能，用于对抗和防御七个攻击阶段。

图 6 - 通过安全功能中断杀伤链



这些功能共同打造了多层防御体系，保护组织免遭威胁侵害并阻止勒索软件传播。

最佳实践

可以采取的措施

仅仅拥有世界一流的深度防御架构还不够。您需要了解对您的企业经营最重要的优先事务，以及系统锁定是否会对其造成影响。

- 最重要的措施是确保您有妥善的备份。如果您每周备份，现在应该改为每天备份；如果每天备份，可考虑改为每小时或实时备份。
- 制定妥善的灾难恢复计划，并确保随着企业的发展和变化定期测试及更新。
- 确定处理重要中断或事件所需的所有人员、流程和工具。执行深入分析，定期测试这些计划。
- 为应用、系统映像、信息和正常运行的网络性能制定全面基线。这些基线可以让您了解网络中的变更，从而能够检测到异常。
- 标准化的操作系统和桌面映像可轻松完成重新映像，从而恢复受感染的基础设施。

发生最坏情况时的恢复

备份恢复是您的最后一道防线，可以避免被迫向攻击者支付赎金的困局。您是否能够以最少的数据丢失和/或服务中断而从攻击中得以恢复，取决于系统备份和/或灾难恢复站点作为攻击者攻击对象的一部分，是否遭到破坏。您的备份是否遭到破坏又取决于备份系统的完善程度和/或网络、恢复站点是否与您的主网络充分进行了分段。即便组织根本不使用现场备份，而是选择使用云备份解决方案（例如 Amazon Glacier），但是如果这些云备份凭证保存在易于获取的位置，或者，如果重复使用密码，那么攻击者就可以轻易地删除所有的备用实例，此时如果没有其他适当的备份解决方案，就会造成 100% 的数据丢失。自认为安全、非现场的企业备份解决方案，如果存在密码重复使用的现象和/或密码管理不善，实际上可以轻易地被攻破。

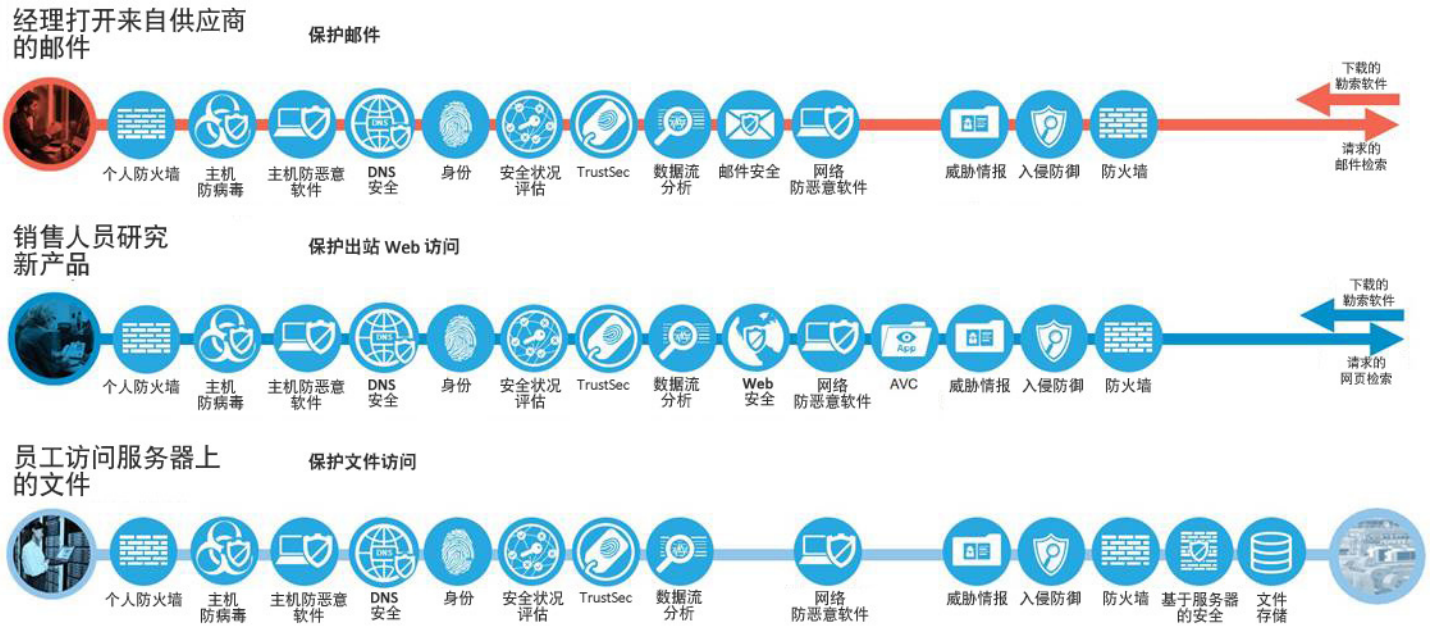
对于使用备份解决方案的企业，有各种各样的备份方法供其选择；SANS 阅览室里有一个关于磁带循环方案的综合性文档非常有用。通常来讲，作为磁带循环策略的一部分，人们会将这些磁带的一部分发送到离站存储设备。这么做的目的是为了进行灾难恢复；如果存放组织数据的站点发生灾难性故障，存储设备里的磁带仍然完好地保存在那里，并可以通过备份设备进行恢复。如果本地备份被删除、撤除或被攻击者使用其他方式导致不可用，如果想不支付赎金，非现场备份通常是恢复服务的唯一希望。您将备份发送至离站的频率，将决定有多少数据（如有）可能发生不可访问或丢失。

解决方案架构

制定深度防御架构的第一步是确定可以中断勒索软件杀伤链的所有功能，并将其与 SAFE 模式中确定的实际业务职能/业务流一一对应。具体对勒索软件而言，就是 Web 浏览和邮件的使用，因为它们是风险最高的感染途径。此外还包括第三种情况，即内部存储中的文件。

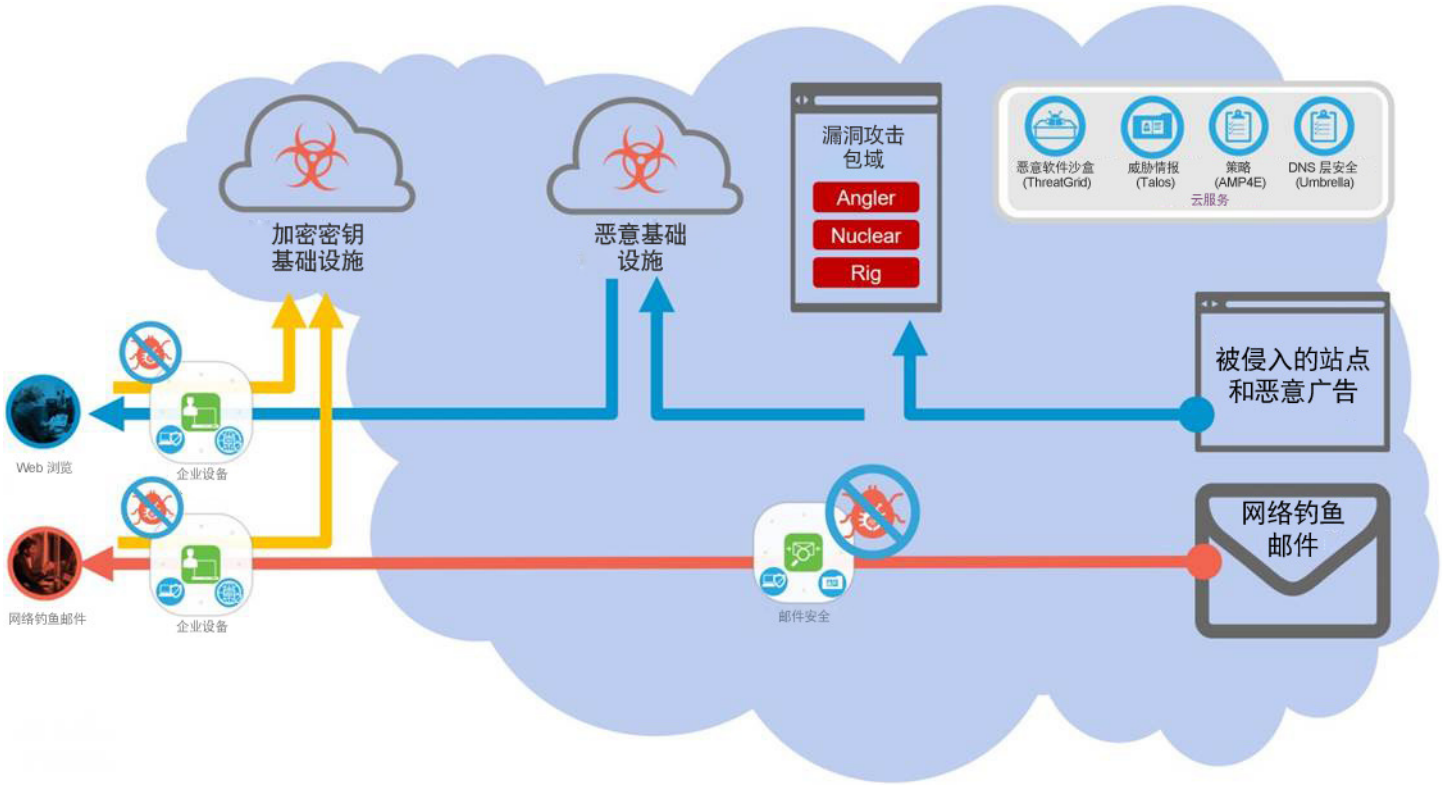
图 7 逐一显示了这三种业务流以及上文所述的选定功能。在整个组织中，这些功能可能在多个网络域中存在重复。图中已删除所有重复项，且这些功能不一定按任何特定顺序排列。它们代表从端到端角度而言保护这些业务流的最佳方式。

图 7 - SAFE 业务流和勒索软件防御功能



由于全面部署这些功能可能需要大量的成本和部署时间，此解决方案已划分为两个阶段。如图 8 所示，第一阶段包括只需相对较少的精力即可快速部署且能显著降低风险的若干功能。第二阶段则会添加剩余的功能，如图 15 中的园区网络架构示例所示。

图 8 - 云和终端功能



第一阶段 - 经过验证的测试

随着勒索软件攻击和感染的威胁迫近，组织必须采取相应的拦截措施，以免沦为下一个受害者。组织必须实施邮件、DNS 和防恶意软件安全功能，借以加强现有安全措施。这些功能都是部署起来既快速又容易的云服务，可以立竿见影地降低被勒索软件攻击得逞的风险。

快速、成功的三个防御步骤包括：

1. 拦截头号感染媒介 - 在邮件附件和 URL 接触到任何一位用户之前对其进行过滤。
2. 阻止命令和控制 (C2) 通信以及恶意站点重新定向 - 增加一层网内和网外 DNS 安全保护。
3. 在所有支持的基础设施（主机、网络、邮件和 Web）中启用恶意文件防护 (AMP) 功能。

部署这些功能至关重要，应按组确定优先顺序（管理员、高管、关键服务器等），并确保尽可能覆盖广泛。

上述每种产品和服务共享基于云的 Talos 威胁情报服务、Threat Grid 文件分析和 Umbrella 安全图。

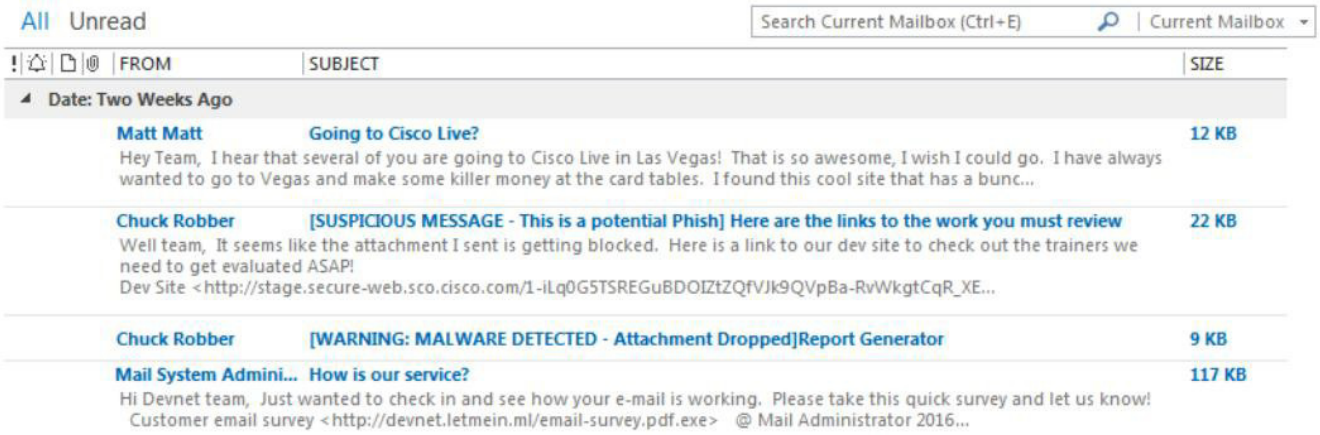
邮件安全

邮件安全功能是在所有邮件传入（红色箭头）组织，在真正接触到可以打开或点击它的人之前，进行预先过滤来拦截大量勒索软件攻击。邮件要经过多个必须启用的策略实施检查步骤的评估。这些步骤包括内容检查、病毒检查、恶意软件检查和欺骗检查。

我们使用高级恶意软件防护 (AMP) 集成服务来执行恶意软件检查。对于已知恶意附件（根据文件散列值和其他识别能力判定），虽然可以只删除附件，但最好是丢弃或隔离整个邮件。对于未知附件，我们将邮件保留在隔离区中，同时在 Threat Grid 文件沙盒服务中对附件进行文件分析。然后，根据返回的分析报告中的严重性选择转发决定。云邮件安全 (CES) 与邮件系统正确集成后，可在其他用户检索到受感染的邮件之前通过追溯功能将该邮件清除。图 9 所示为删除了附件的邮件。

注意：极少数情况下，恶意文件可能最初被分类为“安全”，因为它们能够在分析结束后更改行为。

图 9 - 在主题前面添加通知的邮件



邮件系统还会评估 URL 以确定邮件是否包含垃圾邮件或网络钓鱼链接，然后根据 URL 的信誉执行相应操作。为增强勒索软件防御，还必须全局启用邮件修改和病毒爆发过滤器并将其添加到邮件策略中。病毒爆发过滤器旨在防御各种新型威胁和混合攻击。病毒爆发过滤器可以发布由六种参数（包括文件类型、文件名称、文件大小和邮件中的 URL 等）任意组合构成的规则。

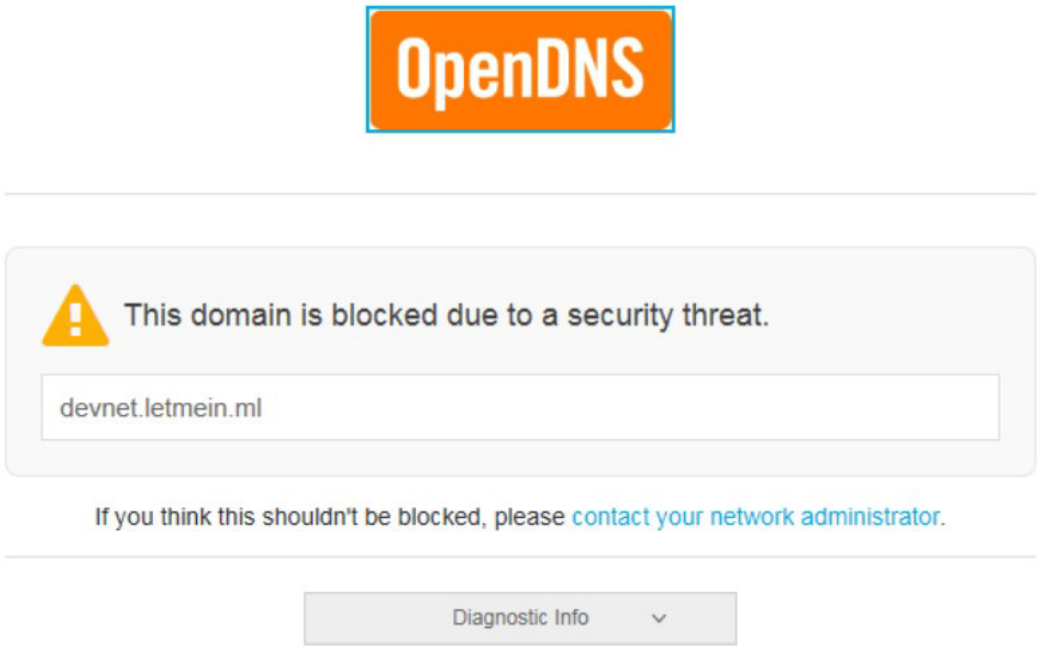
当思科 Talos 威胁情报对病毒爆发事件掌握更多信息后，病毒爆发过滤器会相应地修改规则，并酌情释放隔离区中的邮件。病毒爆发过滤器还能重写可疑邮件中的 URL。通过启用 Web 互动跟踪 (WIT)，可以跟踪这种收件人浏览活动。点击后，新 URL 将通过思科网络安全代理重新定向收件人。然后，系统会主动扫描目标网站的内容，如果该站点包含恶意软件或者会投放勒索软件的漏洞攻击包，病毒爆发过滤器会向用户显示拦截窗口。如果内容未知，则会显示图 10 所示的决策选项。

图 10 - Web 互动跟踪提供的决策选项

DNS 安全

DNS 安全功能在域名解析步骤（将域名转换为 IP 地址，用于访问互联网上的服务器）实施安全措施。此 DNS 层的安全功能有能力在组织网络内部和外部面向所有通信类型保护设备，而不仅仅是保护网站。如果在初次启动时某个 URL 将用户定向至看似可信的站点，无论用户是否点击了链接或是否存在从被侵入的站点重新定向，Umbrella 都会如图 11 所示在用户的浏览器连接到恶意站点前拦截 DNS 请求并将其替换为安全的目的。

图 11 - DNS 拦截页面



如图 11 所示，每个杀伤链阶段（蓝色箭头）可能存在若干不同域的网络，需要为其各自收集不同级别的威胁情报。最初的网络钓鱼站点使用的新域可能只存在数小时或数分钟，而随后的恶意基础设施可能具有数天或数周的已知恶意历史记录。在每个阶段，DNS 安全功能都有机会在入侵发生前拦截通信，从而防止用户受到感染。此外，如果确实发生了感染（黄色箭头），无论使用的端口或协议是什么，Umbrella 也能阻止 C2 回调。这可以阻止勒索软件文件的投放或加密密钥的 C2 回调。

防恶意软件安全

基于主机的防恶意软件功能是最后一道防线，通常也是加密端到端通信（受密码保护的存档、https/sftp、聊天文件传输等）的唯一防御措施。思科的高级恶意软件防护 (AMP) 会分析到达用户系统的所有文件。如果已知文件是恶意的，系统会将其立即隔离，如图 12 所示。

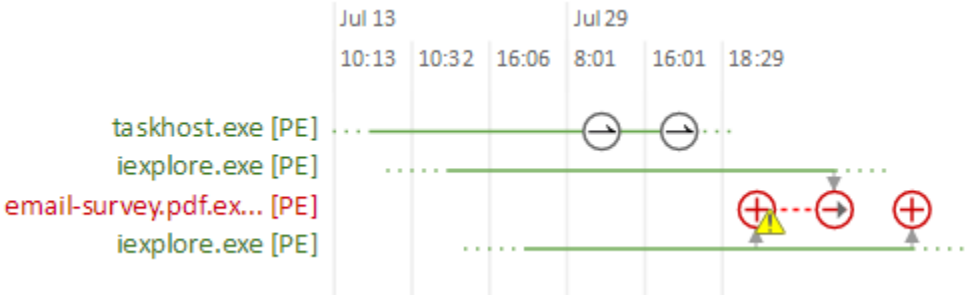
图 12 - AMP 隔离通知

如果文件属于低普遍性（以前从未见过而且没有历史记录的文件），系统会将其自动上传至 Threat Grid 进行分析（需要额外配置和许可），并由其提供追溯性安全功能来检测逃过初始检查的恶意软件。

AMP 结合使用文件签名、文件信誉、行为表现和沙盒分析，可以阻止最初的漏洞攻击包在用户系统上执行，也可以阻止投放的勒索软件文件执行并将其删除。

此外，无论文件的性质如何，AMP 都会持续分析并记录系统中的所有文件活动。如果日后某个文件行为可疑，AMP 可对其进行追溯性检测并发送警报。AMP 会持续记录恶意软件行为的详细历史记录，包括其进入网络的位置和方式、经过的其他位置及其正在执行的操作。然后，AMP 可以根据设置的策略，自动或手动遏制威胁并做出修复。图 13 说明 AMP 如何跟踪文件在系统中的操作。

图 13 - AMP 设备轨迹

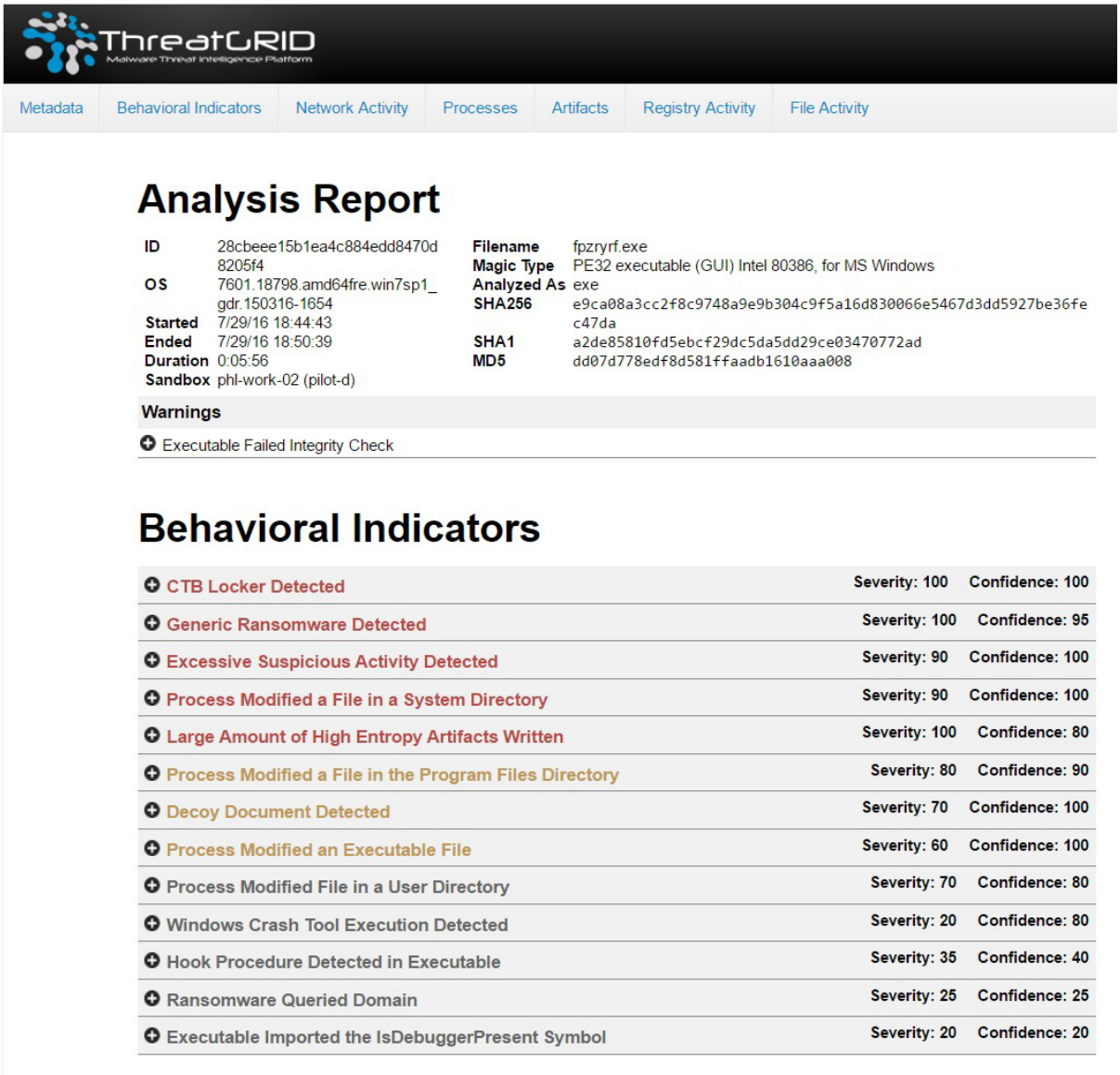


威胁情报

我们的思科 Talos 团队（思科威胁情报团队）每天要分析数百万份恶意软件样本和以 TB 计的数据，并向 AMP 推送情报以提供全天候的防护。此外，高级沙盒功能可以依据 500 多种行为表现对未知文件自动执行静态和动态分析，从而发现隐蔽的威胁。

通过配合使用 Talos 和 Threat Grid 威胁分析引擎，可以在短短 20-30 分钟内对可疑邮件附件和文件进行沙盒测试、分析并分类为恶意软件或勒索软件。不过，低普遍性文件可能需要稍长时间进行分析和识别，才能尽量减少分析时出现误报的可能性。图 14 所示为解决方案验证测试中使用的勒索软件样本的分析报告。

图 14 - 文件分析报告

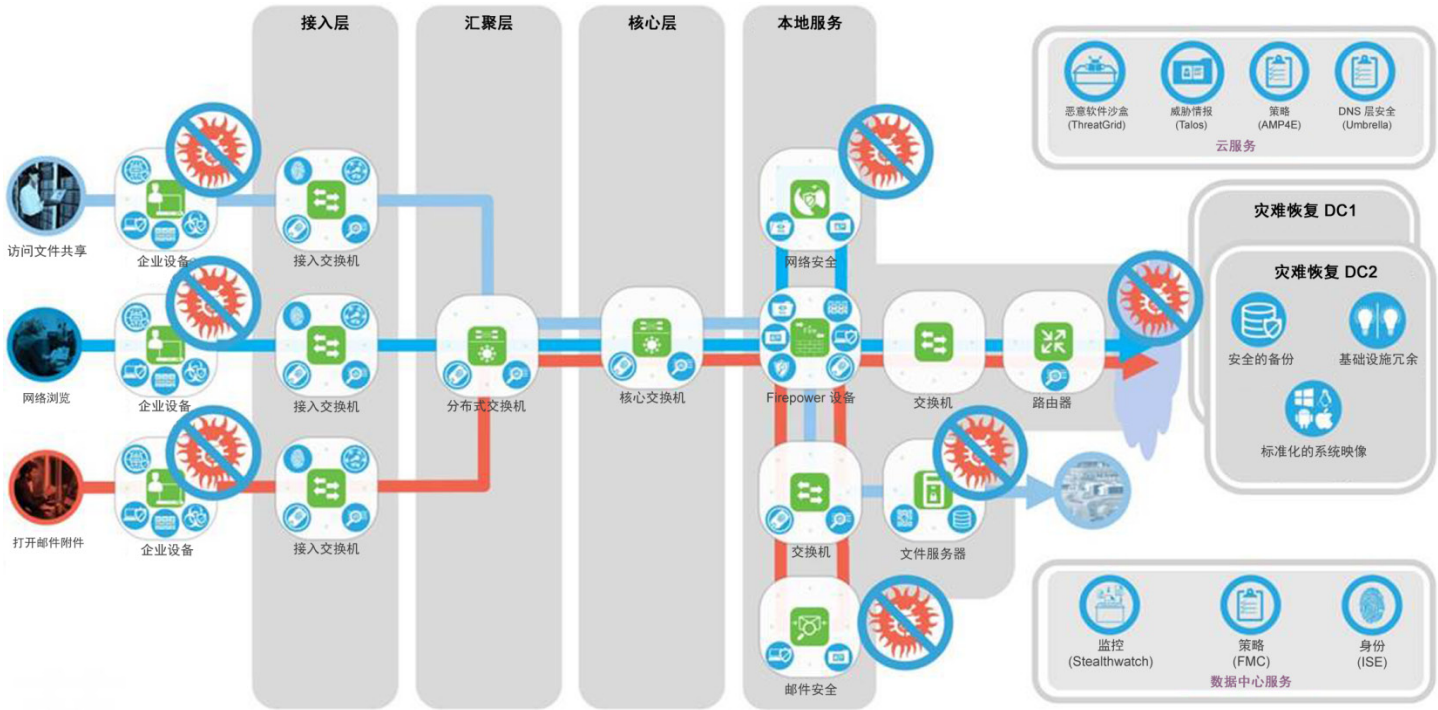


逃过初始检查的恶意软件的追溯性安全情报通过 Talos 威胁情报向邮件和主机防恶意软件服务共享。这些恶意文件当前和未来的所有实例都会受到拦截或删除。

第二阶段 - 园区参考架构

第二阶段架构通过实施完全分段并基于角色的基础设施，以第一阶段部署的功能为基础构建，在整个架构中全面提供网络监控和实施功能。图 15 所示为使用 SAFE 安全园区 PIN 的园区架构示例。业务使用案例的各层沿用上文所用的邮件、Web 和文件共享业务流。保护这些业务流所需的每项功能被应用到相应的系统平台（绿色方块）或显示为云服务。

图 15 - 第二阶段园区架构示例



高级网络安全

通过网络过滤和网络信誉评分，思科网络安全可在一个超过 75 项内容类别的列表中应用过滤器，从而对 5000 多万个已知网站的访问实行控制。这些控制涵盖对网页、各个网页部分和微应用的访问，以便员工能够访问工作所需的网站；并对已知信任域（例如社交网站和其他服务）中挂载的勒索软件应用更加精细的控制和检查。功能包括：

- 基于云和/或本地网络安全网关为所有用户提供保护，不论用户身在何处
- 可将容量从 100 名用户扩展到超过 10000 名用户
- 完全集成的网络安全、应用控制、管理和报告功能
- 由 Talos 威胁情报提供支持，全面实现零日威胁防护

爆发情报在高度安全的虚拟仿真环境中运行网页组件，以确定每个组件的行为以及如何拦截任意恶意软件或勒索软件。

文件信誉功能在文件通过组织网络时捕获每个文件的指纹。我们会将这些指纹发送到 AMP 的基于云的情报网络，以判定信誉。发生攻击后，您可以使用文件追溯功能，跟踪文件进入您的环境后这段时间内的文件性质。如果发现文件是恶意软件，您可以查看文件的进入位置和当前位置，从而减少未来可能发生的入侵。此外，思科感知威胁分析 (CTA) 集成功能可以通过行为分析、异常检测和机器学习主动发现恶意软件感染症状，有助于减少威胁识别时间。

网络监控

思科 Stealthwatch 可在攻击前、攻击中和攻击后为整个组织提供可视性和安全情报。该解决方案持续监控网络，并提供实时威胁检测和勒索软件爆发时的事件响应调查分析。

Stealthwatch 将网络转变为传感器，从基础设施和工作站采集 NetFlow 数据并进行分析，确定组织及其用户的正常通信基线。根据这条基线，当经验老道的攻击者渗入网络试图分析和部署勒索软件时，就能更加容易地发现他们。它能够识别各种恶意软件、分布式拒绝服务 (DDoS) 攻击、高级持续性威胁 (APT) 和内部威胁。它会同时监控北-南流量和东-西流量（横向流量）的活动情况，因此可以识别更广泛的攻击类型。

Stealthwatch 与思科身份服务引擎和思科 TrustSec 技术结合使用。您可以通过此集成识别用户和系统，并根据系统行为自动对重要的网络资产进行适当分段。

基于身份进行分段

为了最有效地防止勒索软件传播，应该只允许用户访问其履行职责所需的资源和系统文件共享。感染勒索软件的系统会尝试搜索网络中的其他文件共享驱动器和存在漏洞的系统，以便使用当前系统用户的凭证加密或感染这些设备。

采用思科身份服务引擎 (ISE) 的思科 TrustSec 用于对您的网络进行分段并实施基于角色的访问控制。采用思科 TrustSec 技术，可以依照特定的安全策略，按情景、用户、设备和位置控制对网段和资源的访问。

实施安全组标记 (SGT) 后，系统可阻止具备维护承包商凭证的受感染用户系统访问财务数据，不管网络拓扑是什么，或承包商是使用有线还是无线网络接入都是如此。

通过与 Stealthwatch 集成，当根据网络中的异常行为发现受感染系统后，身份服务引擎可以根据获知的此行为发起授权变更，并应用不同的 SGT 策略将这些系统隔离，让网络的其余部分即时获得保护。

基础设施分段和入侵防御

通过 NGFW 进行分段

思科 Firepower 下一代防火墙 (NGFW) 是专注于威胁防御的下一代防火墙，它将多种功能完全集于一身，并且支持统一管理。从网络到终端，NGFW 可以为防火墙功能、应用控制、威胁防御和高级恶意软件防护提供全面的统一策略管理，其中每一项都能提供更多的或备用的勒索软件威胁防御层。

当组织成为勒索软件攻击的目标时，上述各项功能可以协同工作，共同抵御网络侦测。通过阻止各种网络资源之间的通信，可以按照业务通信的需要，将基础设施划分给允许的用户、系统和协议，并阻止那些用于渗入网络、利用漏洞、泄露数据或检索加密密钥以及在网络中存留的通信。

Firepower NGFW 可以实现全面的策略管理，控制访问、阻止攻击、抵御恶意软件，并提供集成工具来跟踪已遭受的攻击、遏制攻击和从攻击中恢复。

通过 Firepower 管理中心进行管理

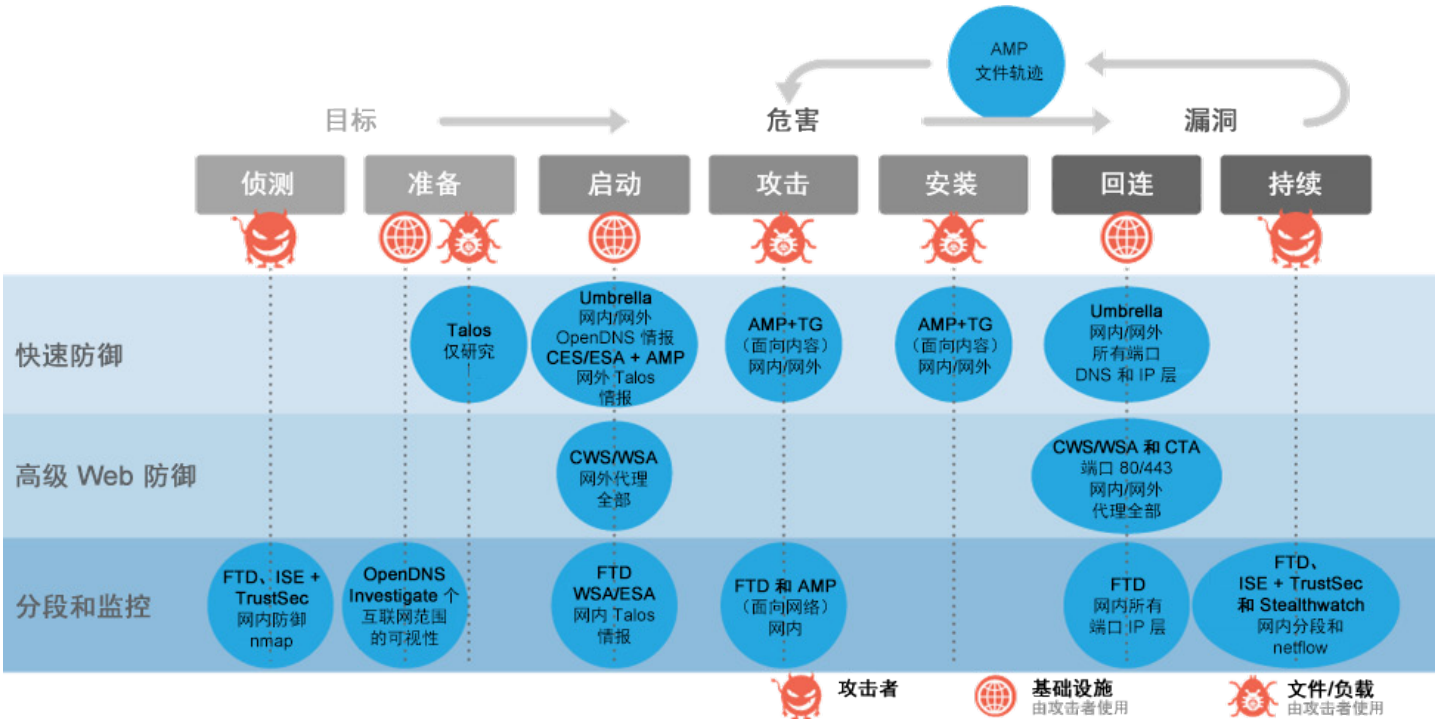
这是用于网络安全管理的管理中枢。它可以在防火墙平台上对防火墙、应用控制、入侵防御、URL 过滤和高级恶意软件防护进行全面、统一的管理。从防火墙管理过渡到应用控制，乃至勒索软件爆发调查与补救，都能在这个单一平台上轻松实现。

借助思科 Firepower 管理中心和 Stealthwatch 行为分析，您可以共享安全情报并通过 ISE 自动执行威胁遏制。

架构总结

上文各阶段中提及的每种产品都能满足在整个杀伤链中防御攻击所需满足的功能要求（如图 16 所示）。

图 16 - 杀伤链中的产品替换功能



实施和验证

表 3 列出了为勒索软件防御解决方案验证测试所实施的产品。有关产品的每节内容分别介绍了如何在典型安装后进行自定义才能最有效地防御勒索软件。

表 3 - 进行验证的解决方法产品

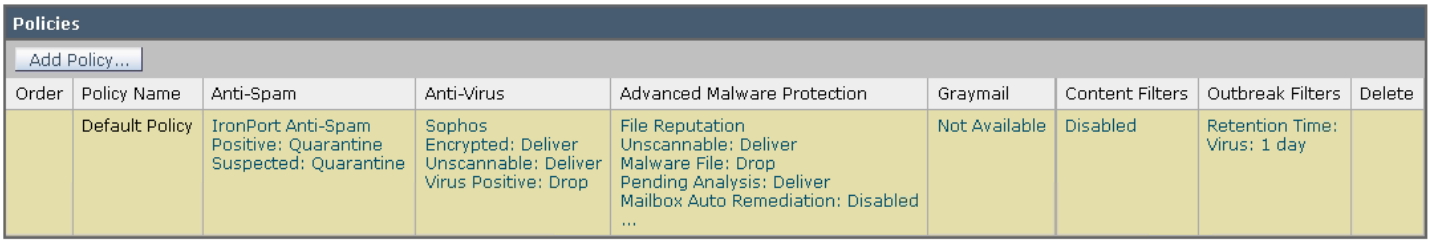
产品	说明	平台	版本
云邮件安全	采用 AMP 的邮件安全设备	云	v10.0.0-071
Umbrella Roaming 和基于网络的 DNS 保护	面向组织外部的漫游用户的 DNS 安全解决方案。面向所有内部设备和系统的网络 DNS	云/漫游客户端	v2.0.189
高级恶意软件防护 (AMP)	面向终端的主机防恶意软件防护	云/客户端终端	v4.4.2.10200

思科云邮件安全

以下步骤概述在云邮件安全服务启动并正常运行且完全集成到您的邮件流程中之后，如何配置邮件安全才能最有效地防御勒索软件和其他高级持续性威胁 (APT)。对于新安装的 CES，默认策略应与下面的图 17 类似。

步骤 1　　依次选择“邮件策略”>“传入邮件策略”。

图 17 - 新部署的默认策略



在传入邮件策略中，我们需要编辑级恶意软件防护、内容过滤器和病毒爆发过滤器的默认策略元素。

高级恶意软件防护。

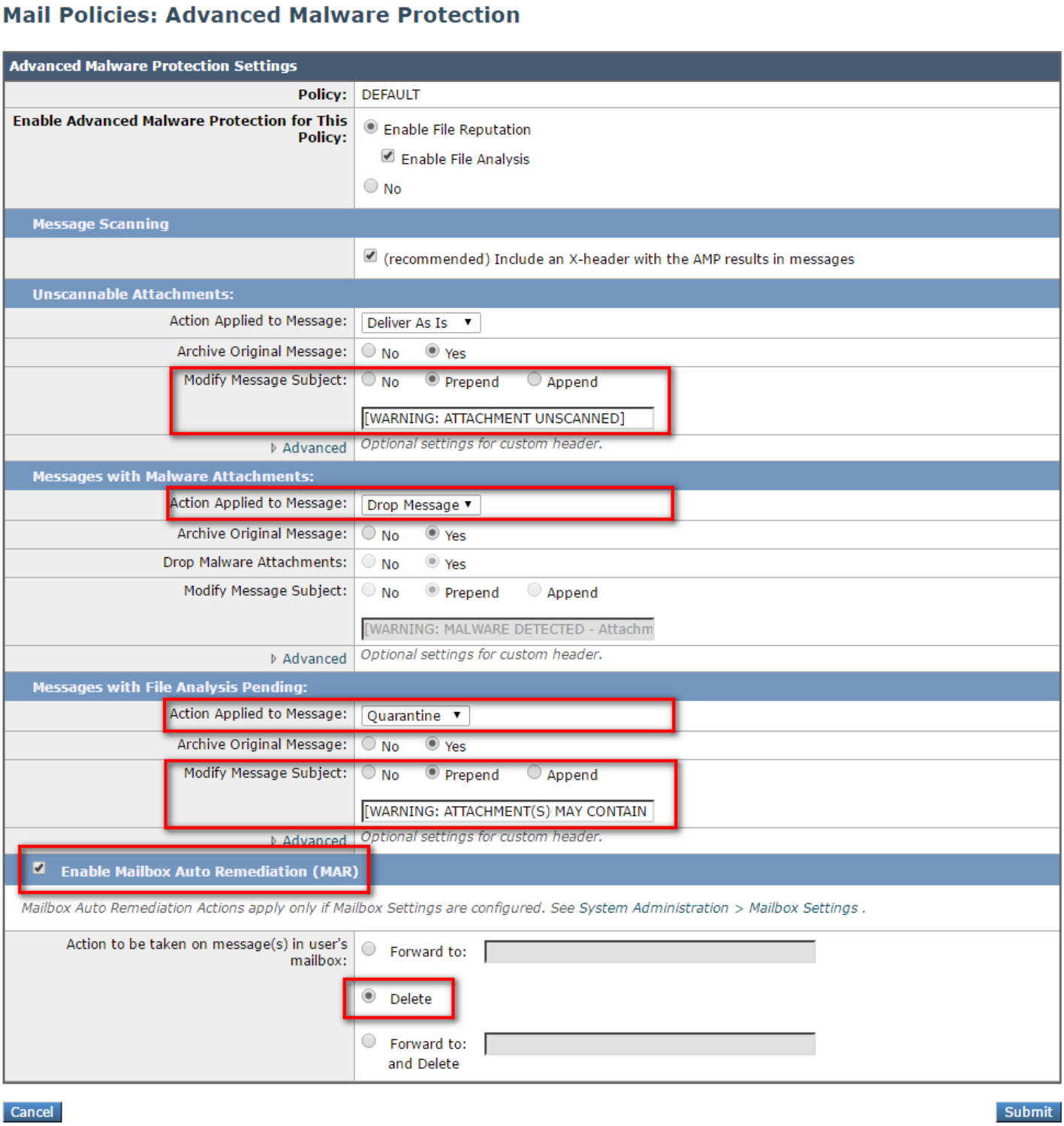
高级恶意软件防护通过如下方式防范邮件附件中的零日威胁和基于文件的针对性威胁：

- 获取已知文件的信誉
- 分析尚不为信誉服务所知的某些文件的行为
- 在获得新信息时持续评估新出现的威胁，并在确定为威胁的文件进入您的网络后通知您

这些功能仅可用于传入邮件。不评估附加到传出邮件的文件。

步骤 1 点击“默认策略”的“高级恶意软件防护”列中的链接对其进行修改。

图 18 - 默认策略中的高级恶意软件防护



最好是根据邮件附件的状态，在邮件主题的前面添加说明性的警告。

步骤 2 为“无法扫描的附件”和“文件分析待定”这两种结果配置“修改后的邮件主题”。

对于包含恶意软件附件的邮件，可以删除附件、附带警告地投递或将邮件连同附件一起丢弃。最常见的做法是丢弃整个邮件。

步骤 3 依次配置“应用于邮件的操作”>“丢弃邮件”。

对于文件分析结果待定的邮件，可以投递也可以隔离。最好是隔离这些邮件，直至分析引擎收到结果。如果附件是恶意的，邮件将按附件设置处理。如果返回的结果是未知，系统将投递该邮件，并在邮件主题前面添加警告。

步骤 4 依次配置“应用于邮件的操作”>“隔离”。

通过启用邮箱自动补救 (MAR)，可以在威胁判定稍后更改为恶意的情况下，删除已经投递到用户邮箱的邮件。

步骤 5 通过选中“启用”配置 MAR，并将操作设置为“删除”。

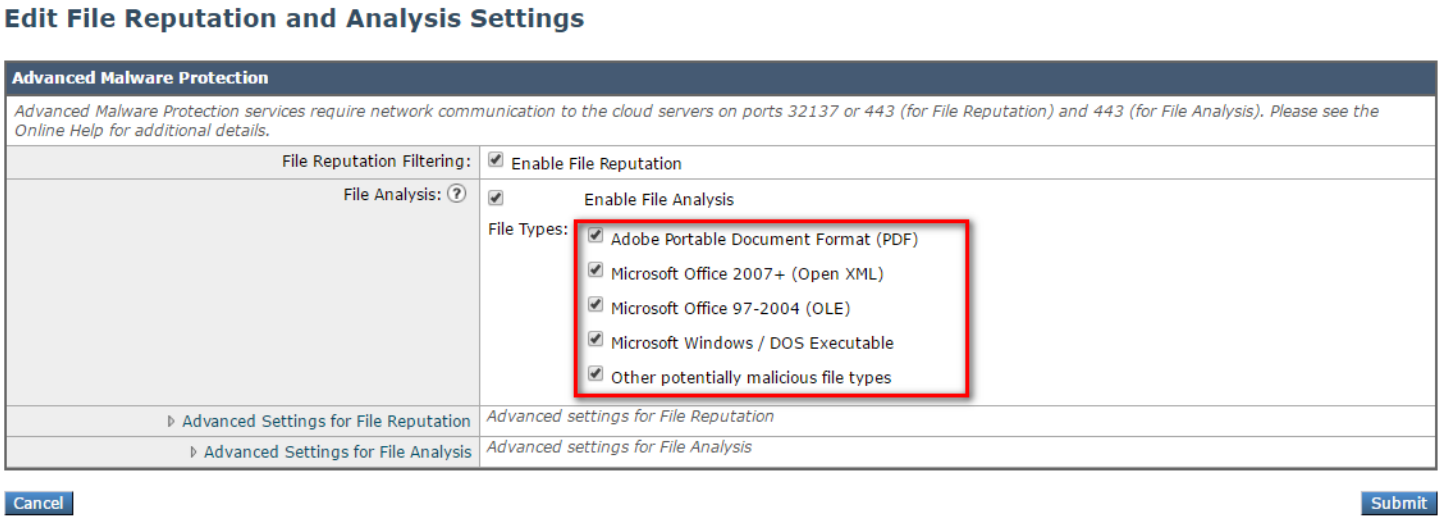
步骤 6 完成这些更改后，点击“提交”。

上面的策略启用文件信誉和分析服务后，该服务将实施 AMP 引擎以对邮件进行检查。文件分析是新实施默认启用的功能，它会检查 Windows 和 DoS 可执行文件，但是您还应该选择其他要分析的文件类型。

步骤 7 依次选择“安全服务”>“文件信誉和分析”。

步骤 8 选择“编辑全局设置”

图 19 - 文件分析设置



步骤 9 如上面的图 19 所示，启用其他文件类型。点击“提交”。

内容过滤

有些勒索软件和漏洞攻击包作为脚本附加到邮件中，因此文件分析不会对其进行检查。如果在 Web 浏览器中打开这些脚本并绕过安全功能，这些脚本就可以在系统上本地运行。
思科建议，最好是使用内容过滤删除以下类型的脚本附件：

- .js
- .wsf
- .vbs

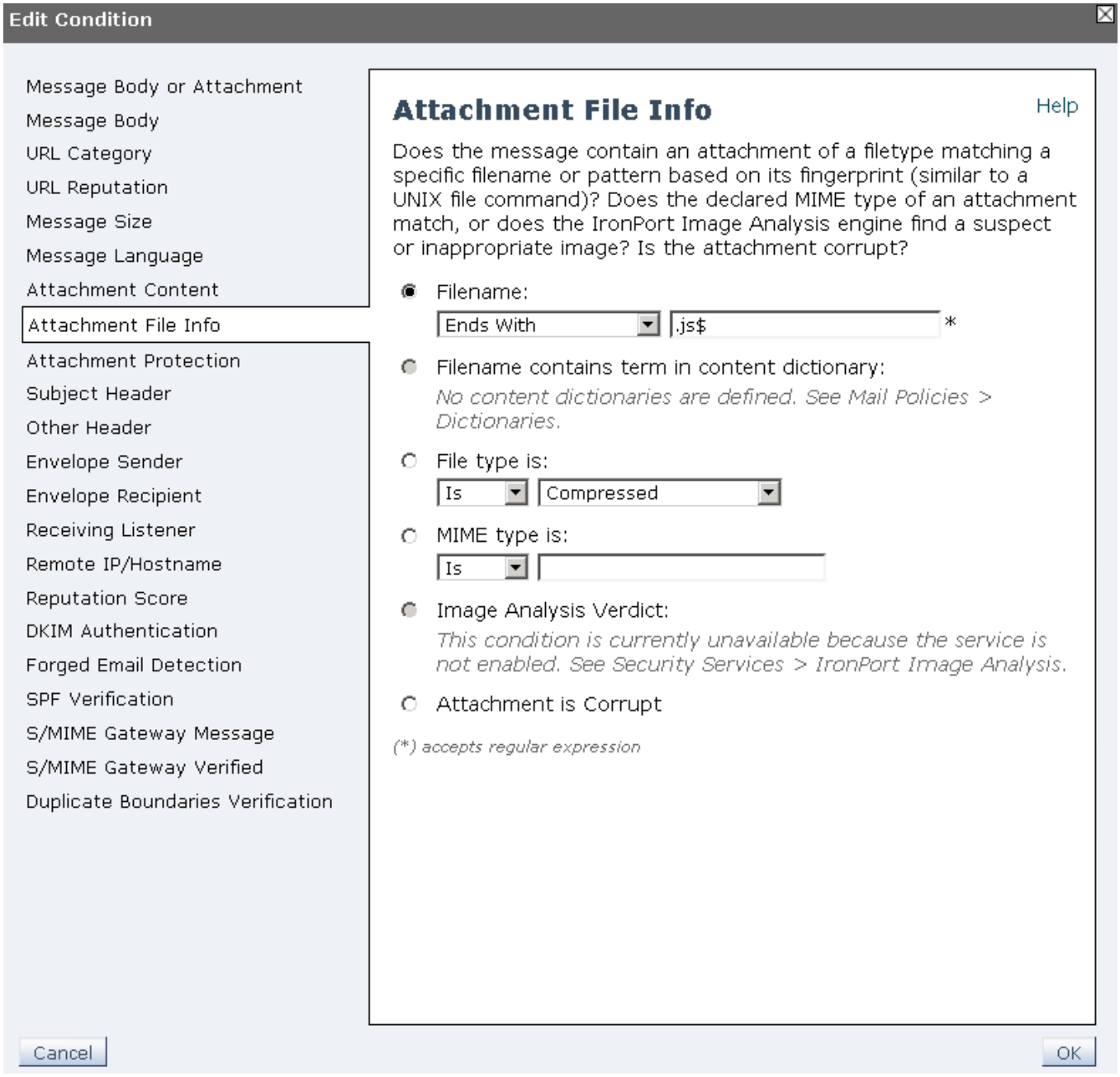
创建新的传入内容过滤器，丢弃包含这些附件的邮件。

步骤 10 依次选择“邮件策略”>“传入内容过滤器”>“添加过滤器”。

步骤 11 输入描述性名称和说明。
名称：BlockScriptAttachments
说明：通过拦截以下脚本附件帮助用户防御勒索软件：.js、.wsf 或 .vbs

步骤 12 依次点击“添加条件”>“附件文件信息”>“文件名包含 .js”。

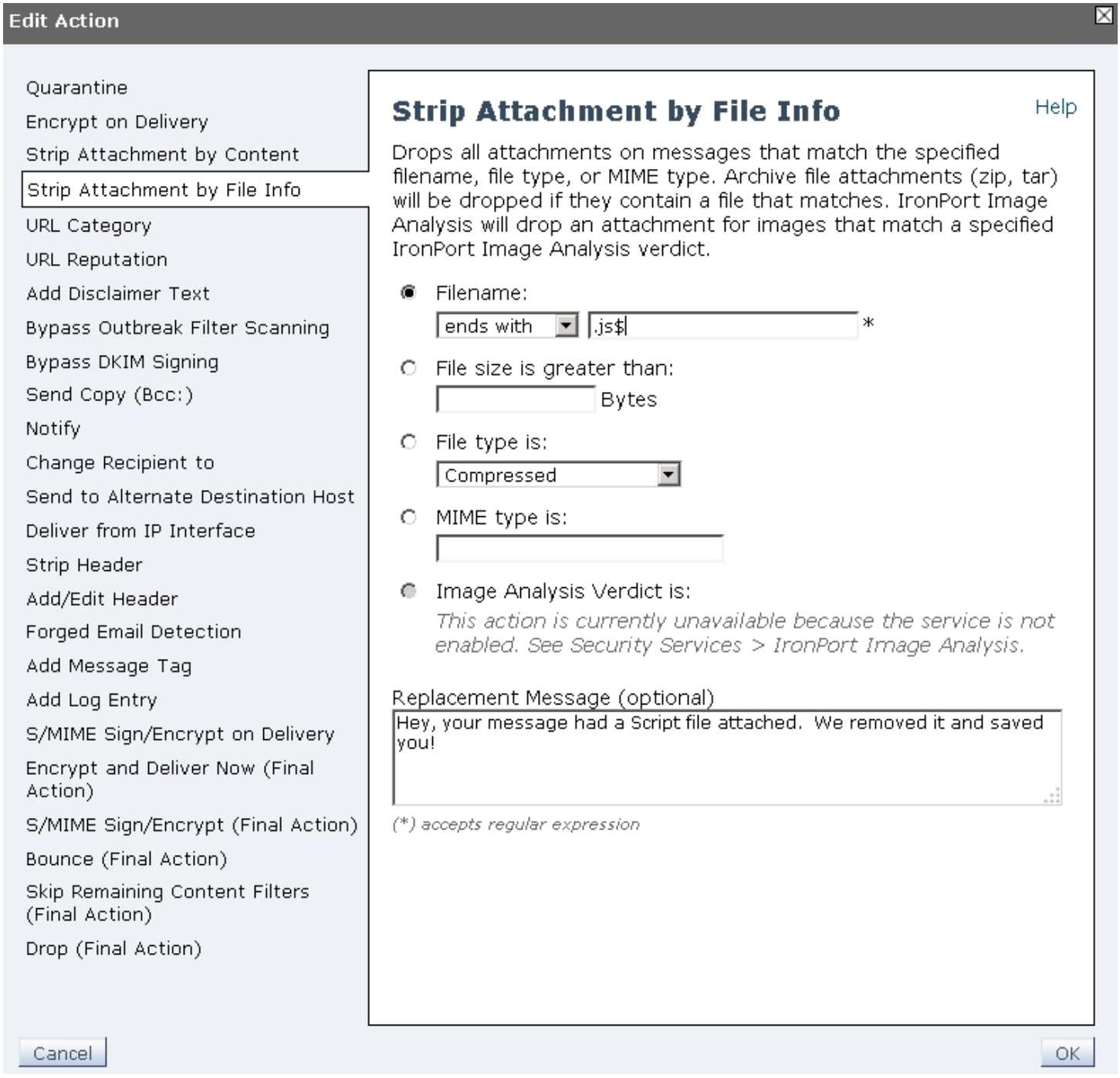
图 20 - 新建内容过滤器条件



步骤 13　　点击“确定”。

步骤 14　　依次点击“添加操作”>“按文件信息删除附件”>“文件名包含 .js”。

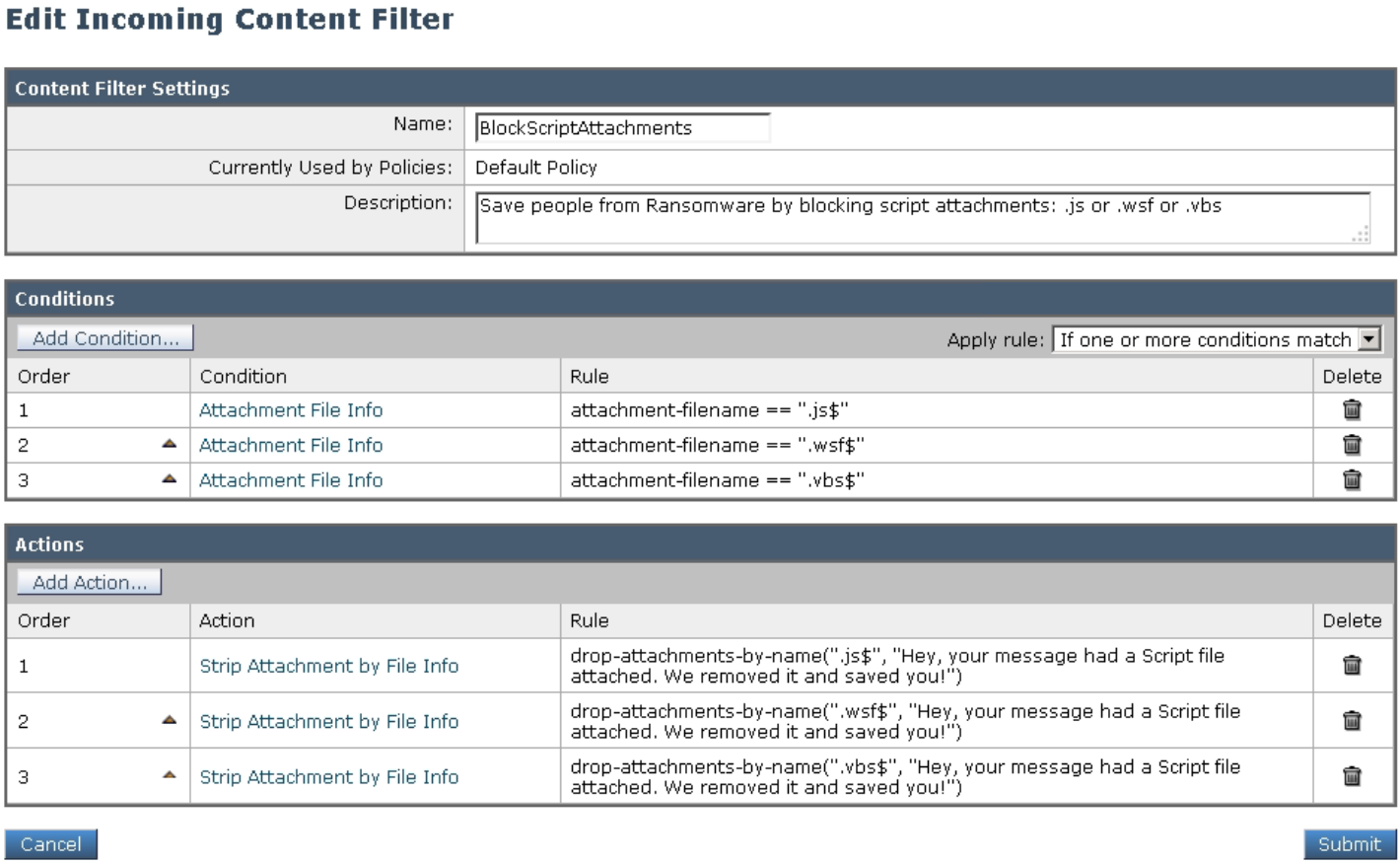
图 21 - 新建内容过滤器操作



步骤 15　　点击“确定”。

对 .wsf 和 .vbs 文件类型也重复步骤 12-15。最终的过滤器应包含图 22 中所示的全部六项设置。

图 22 - 用于删除脚本文件的内容过滤器



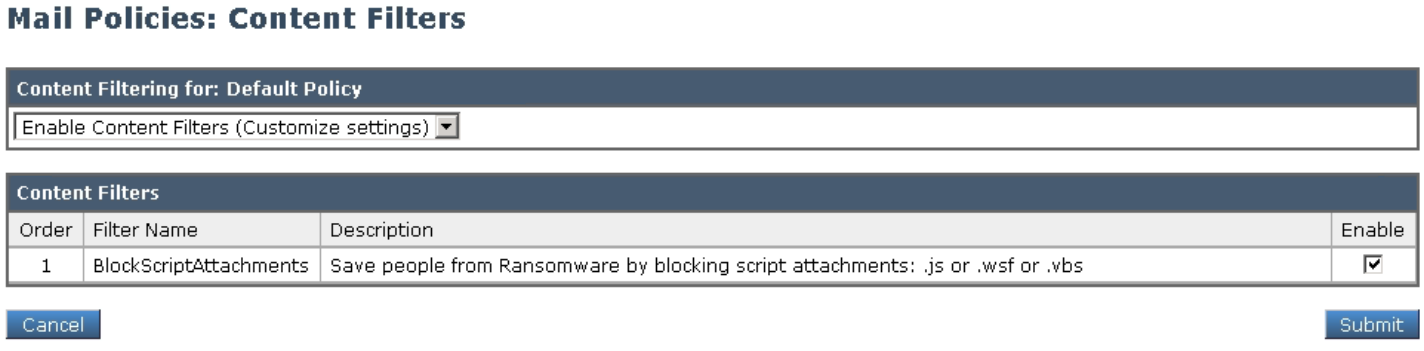
步骤 16　　完成后，点击“提交”。

在“默认策略”中启用新的“内容过滤器”

步骤 17　　依次选择“邮件策略”>“传入邮件策略”>“默认策略”的“内容过滤器”列中的“禁用”对其进行修改。

步骤 18　　从下拉列表中选择“启用内容过滤器”，选中新创建的过滤器的“启用”列。

图 23 - 启用内容过滤和过滤器



步骤 19　　完成后，点击“提交”。

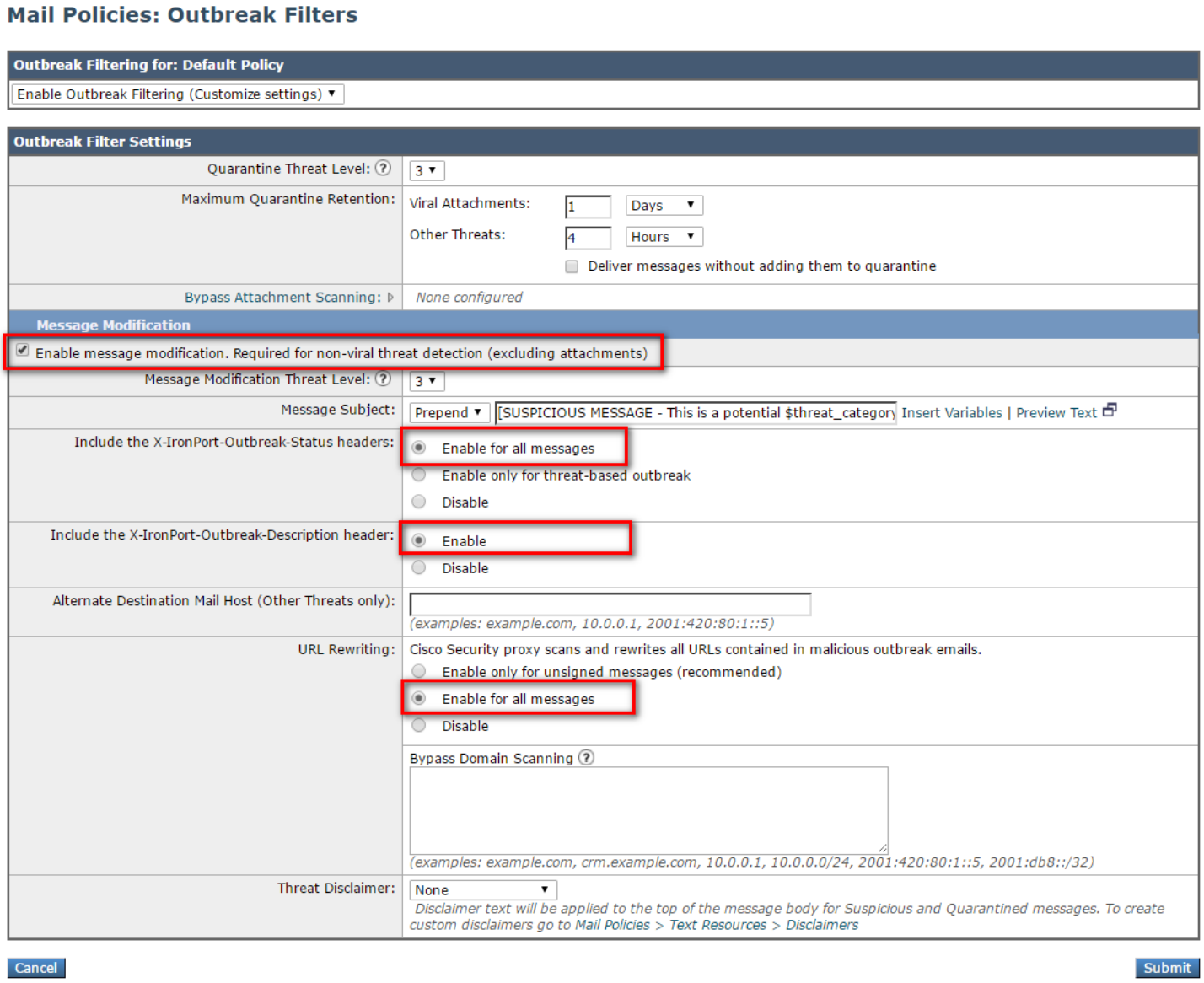
病毒爆发过滤器

病毒爆发过滤器既能保护您的网络免受大规模病毒爆发，又能在出现小规模非病毒攻击时防御它们，例如网络钓鱼、诈骗和恶意软件传播。思科会在病毒扩散时收集有关病毒爆发的数据，并实时更新威胁情报服务，从而防止这些邮件接触到您的用户。

对于全新安装，病毒爆发过滤器默认启用，但最好同时还启用邮件修改功能，它可以对邮件进行 URL 重写。在打开特定邮件时，此功能会通知用户谨慎处理。

步骤 20　依次选择“邮件策略”>“传入邮件策略”>“默认策略”的“病毒爆发过滤器”列中的“保留时间”对其进行修改。

图 24 - 病毒爆发过滤器的邮件通知



步骤 21　启用邮件修改完毕后，点击“提交”。

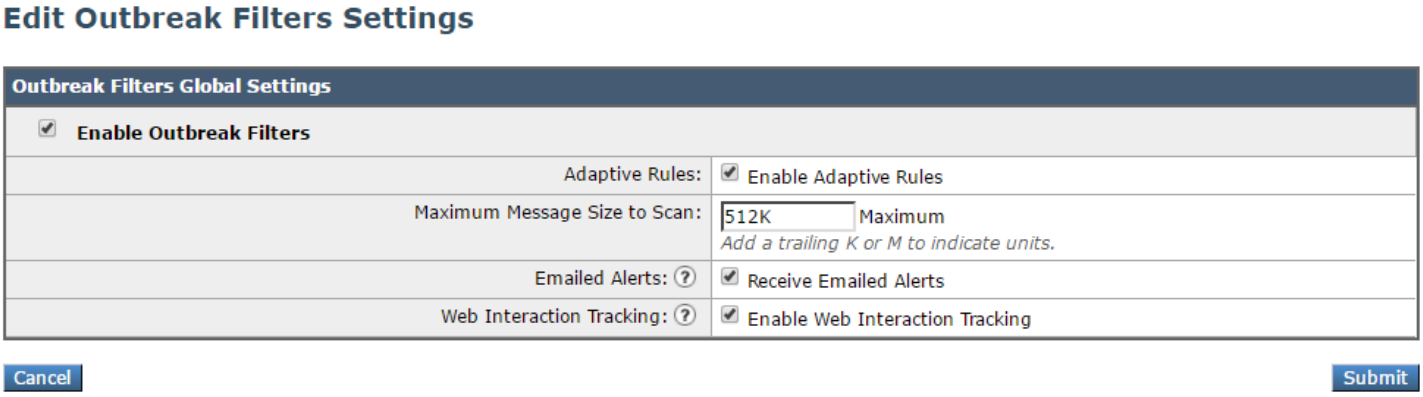
Web 互动跟踪

借助 Web 互动跟踪，管理员可以跟踪点击思科邮件安全设备重写过的 URL 的终端用户。可以跟踪包含恶意链接的邮件，包括点击该链接的用户及其操作造成的结果。

默认情况下，Web 互动跟踪处于禁用状态。要跟踪因病毒爆发过滤器而重写的 URL，必须启用 Web 互动跟踪。

步骤 22 依次选择“安全服务”>“病毒爆发过滤器”>“编辑全局设置”

图 25 - 用于病毒爆发的 Web 互动跟踪

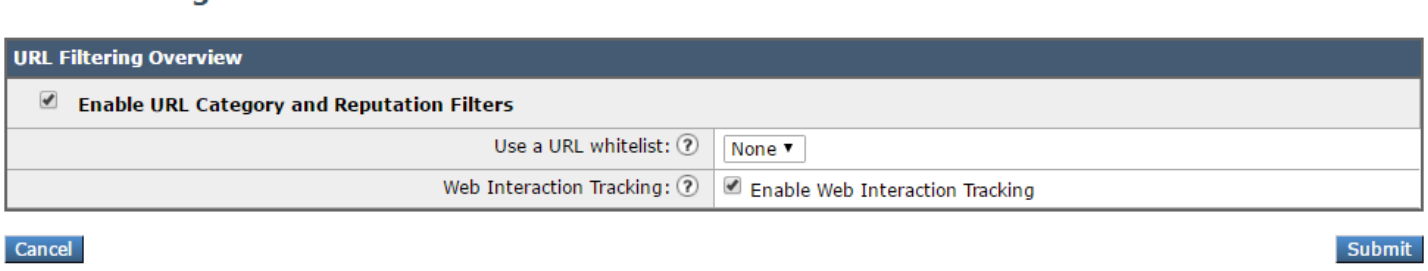


步骤 23 选中“邮件警报”和“Web 互动跟踪”复选框。然后点击“提交”。

如果还要跟踪因策略而重写的 URL，您还必须在 URL 过滤设置中启用 Web 互动跟踪。

步骤 24 依次选择“安全服务”>“URL 过滤”>“启用”。

图 26 - 用于 URL 过滤器的 Web 互动跟踪



步骤 25 选中“启用 URL 类别和信誉过滤器”和“启用 Web 互动跟踪”复选框，然后点击“提交”。

完成所有更改后，需要提交更改才能使这些新设置生效。

步骤 26 点击右上角的黄色“提交更改”按钮，留下适当的注释，然后点击“提交更改”提交。

思科 Umbrella DNS 安全

Umbrella Roaming 客户端可为笔记本电脑提供保护，无论这些电脑位于何处或如何连接到互联网。该客户端的工作方式如下：通过遍布全球的 OpenDNS 全球网络数据中心之一，安全地将互联网的 DNS 查询绑定重新定向至 Umbrella 安全云网关，从而按照您的选择实施策略并应用安全功能，防止计算机遭到入侵。

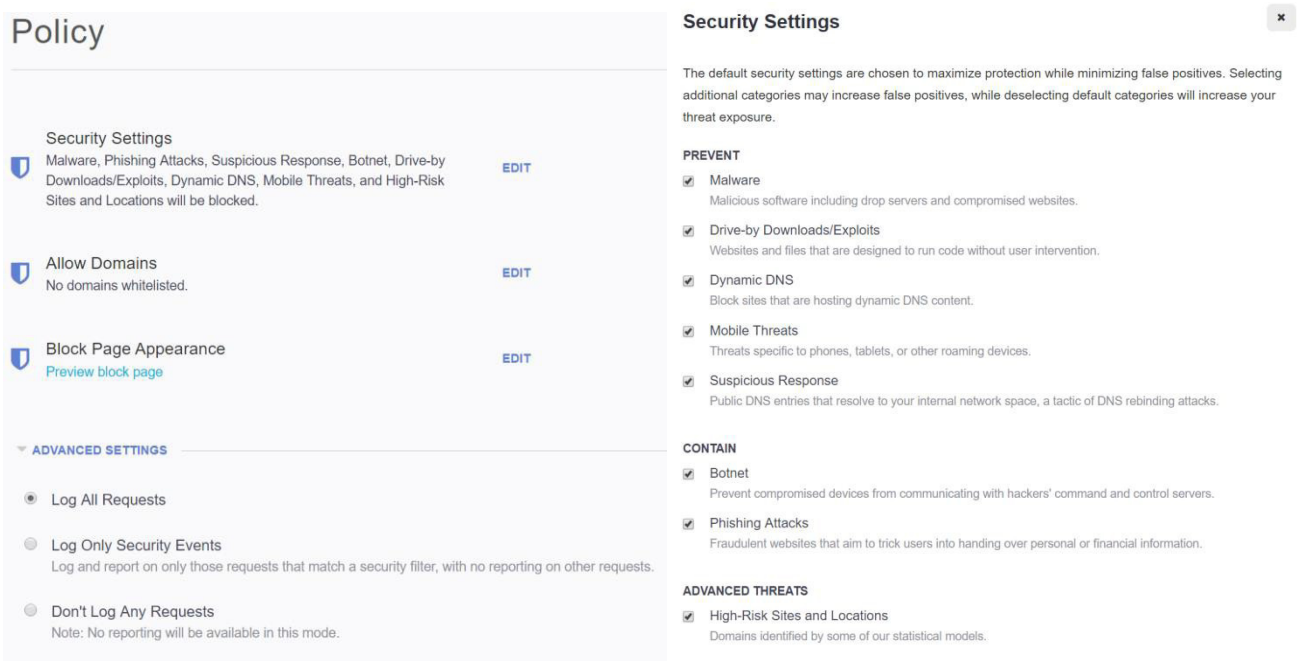
适用的若干场景包括通过 3g/4g 无线运营商网络访问互联网的计算机、经 Wi-Fi 热点（例如机场、咖啡厅、酒店，家中）接入的不可信网络，以及位于可信的网络网关后的办公环境或受到 Umbrella 保护的网络中。

无需完成额外的配置步骤即可实现勒索软件防御。有关下载和安装漫游客户端的程序，请访问：
http://info.umbrella.com/rs/opendns/images/TD-Umbrella-Mobility-Roaming-Client-Guide.pdf

思科 Umbrella Roaming

如图 27 所示，仅提供思科 Umbrella Roaming 的产品使用的是简化的策略，只阻止重要的安全威胁。

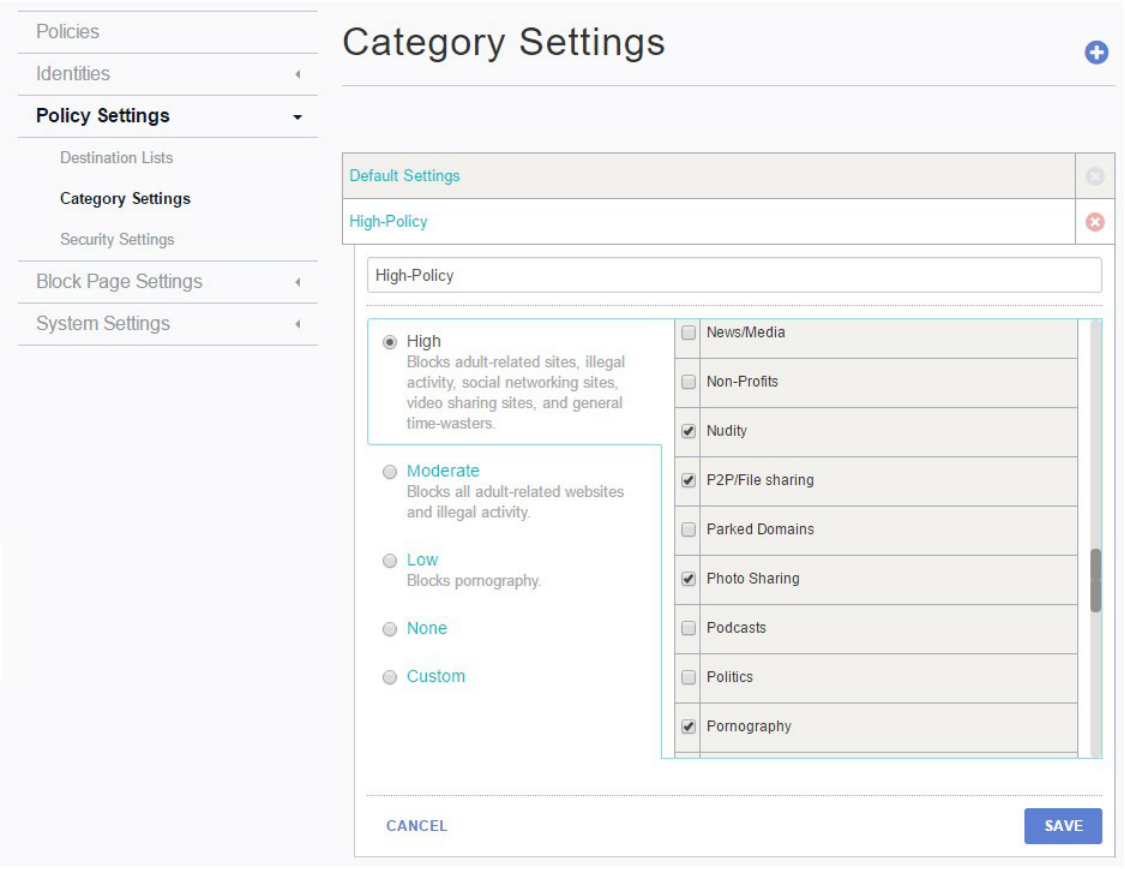
图 27 - 思科 Umbrella Roaming 的计算机策略



思科 Umbrella

完整的思科 Umbrella 产品可为网络、漫游和移动设备提供保护。该产品包括一组更加全面的策略选项，其中包括限制访问其他类别的内容，这些内容同样可以降低被定向至可能托管着勒索软件的域的风险（例如赌博、P2P/文件共享、仇恨/歧视）。除了创建自定义策略外，还有若干预配置策略可用。图 28 显示了验证测试中使用的“高策略”。

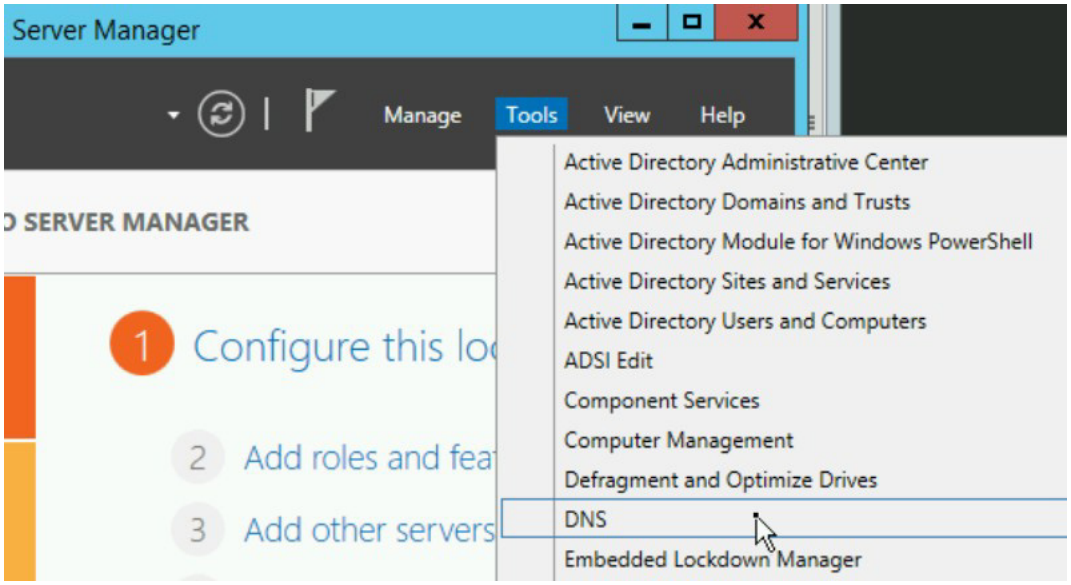
图 28 - Umbrella 高策略



对于自行实施内部网络 DNS 服务器的组织而言，可以为整个网络轻松启用 Umbrella。请将 DNS 服务器配置为使用 Umbrella 服务器作为转发器，而非自行对外部域执行根查询。这样就无需在任何内部网络系统上部署 Umbrella 客户端，从而实现简单的无客户端实施，保护网络中的一切。以下步骤概述如何像我们在验证测试过程中执行的那样，将 Windows DNS 转发配置为使用 Umbrella。

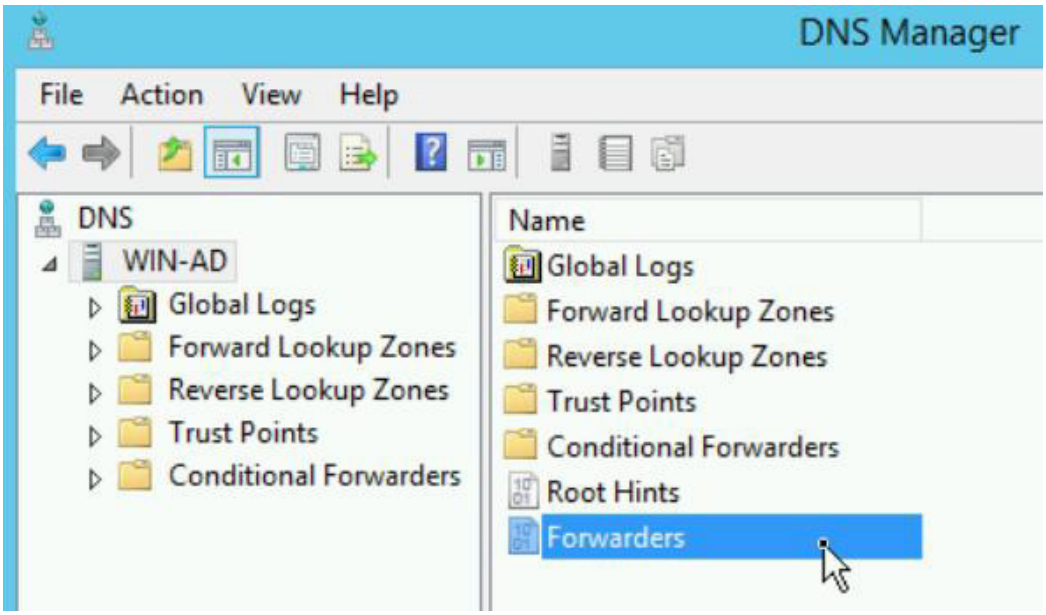
步骤 1 在服务器工具下，打开 Windows DNS 管理器。

图 29 - Windows DNS 管理器



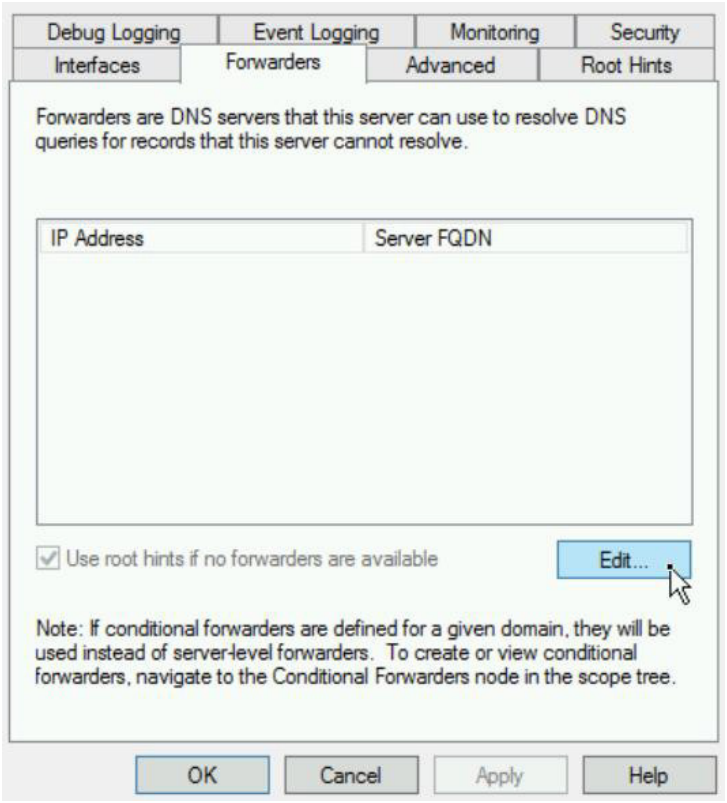
步骤 2 选择要编辑的服务器，然后选择“转发器”。

图 30 - Windows DNS 管理器转发器



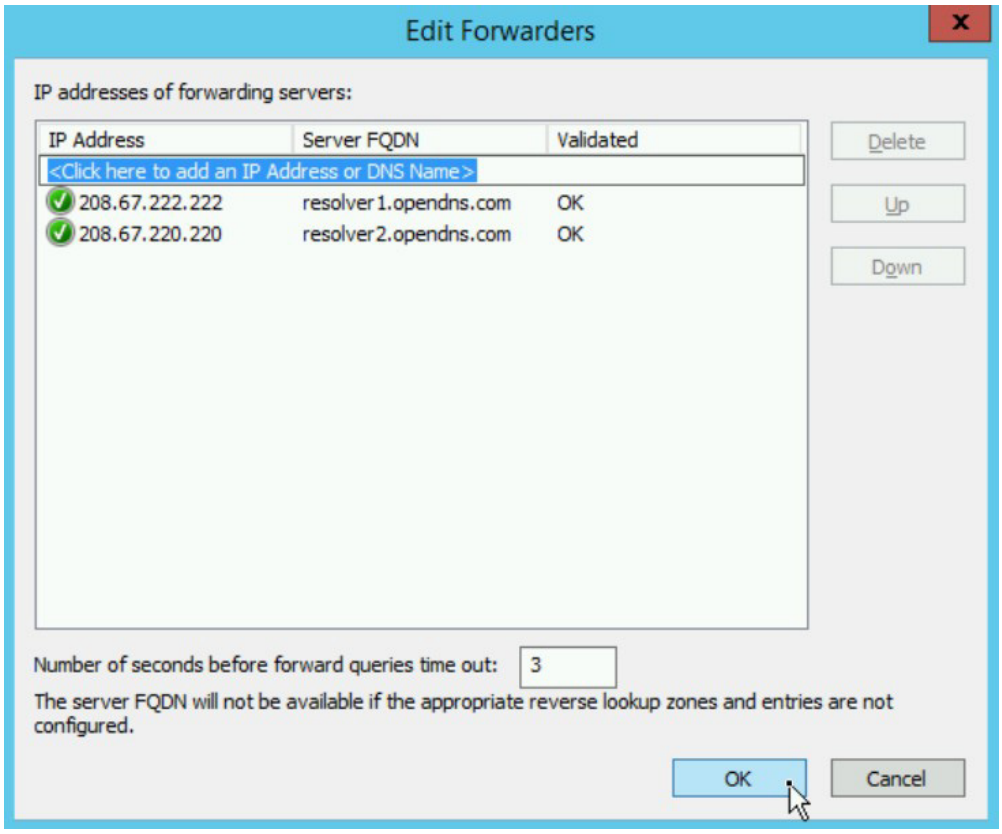
步骤 3 点击“编辑”。

图 31 - 编辑 Windows DNS 转发器



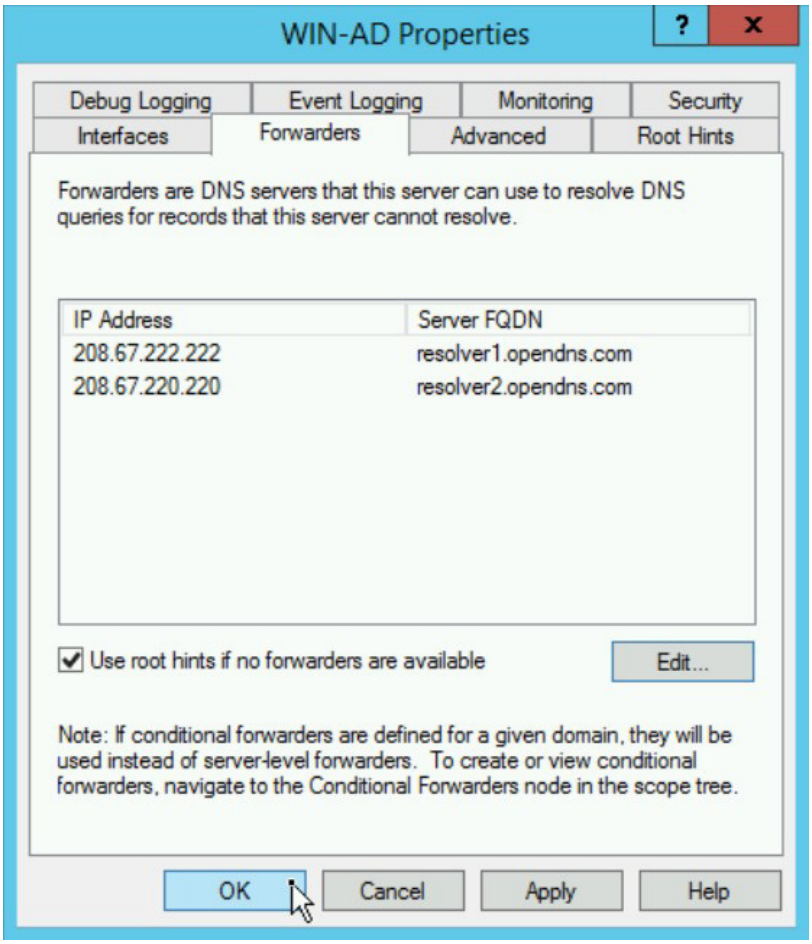
步骤 4 输入 Umbrella DNS 服务器的地址 208.67.220.220 和 208.67.222.222，然后点击“确定”。

图 32 - 添加 Windows DNS 转发器



步骤 5 点击“确定”提交更改并关闭配置窗口。

图 33 - 完成对 Windows DNS 管理器的更改



将 DNS 服务器使用的公有 IP 地址添加到 Umbrella 中的网络身份中。

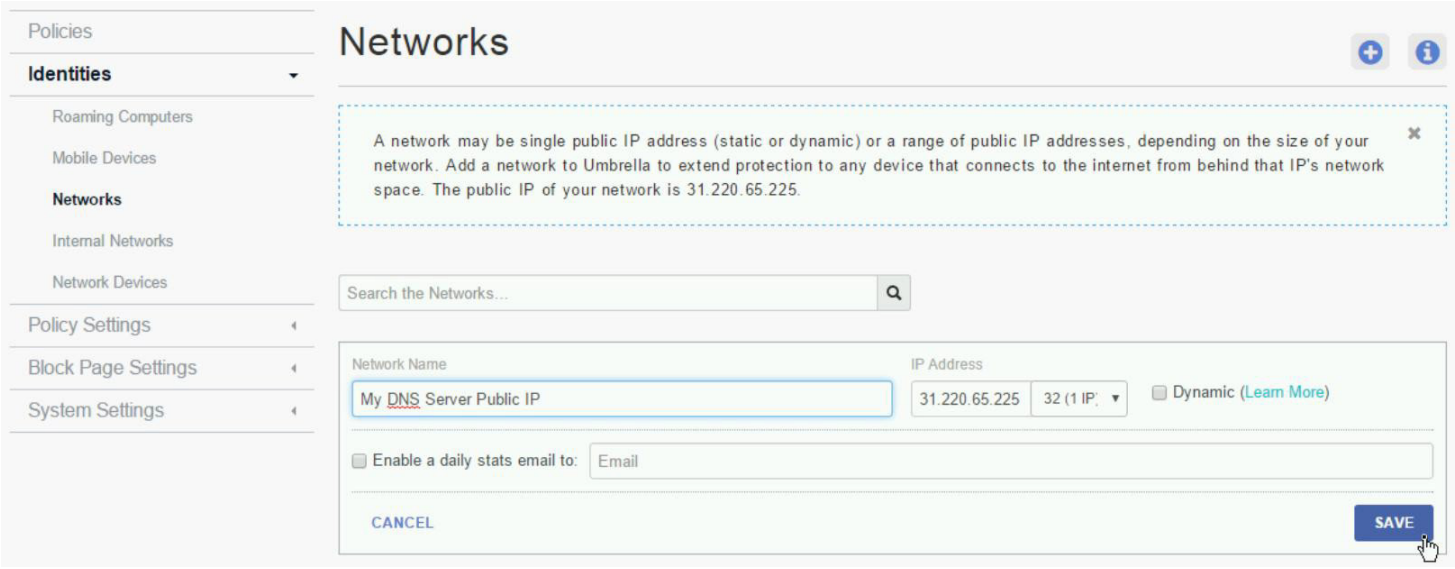
步骤 6 依次选择“配置”>“身份”>“网络”。

步骤 7 点击加号图标添加新的网络。

图 34 - 添加 Umbrella DNS 网络

步骤 8 输入该网络的公有 IP 地址以及子网掩码（通常是一个 /32 子网）并选择一个描述性名称。然后点击“保存”。

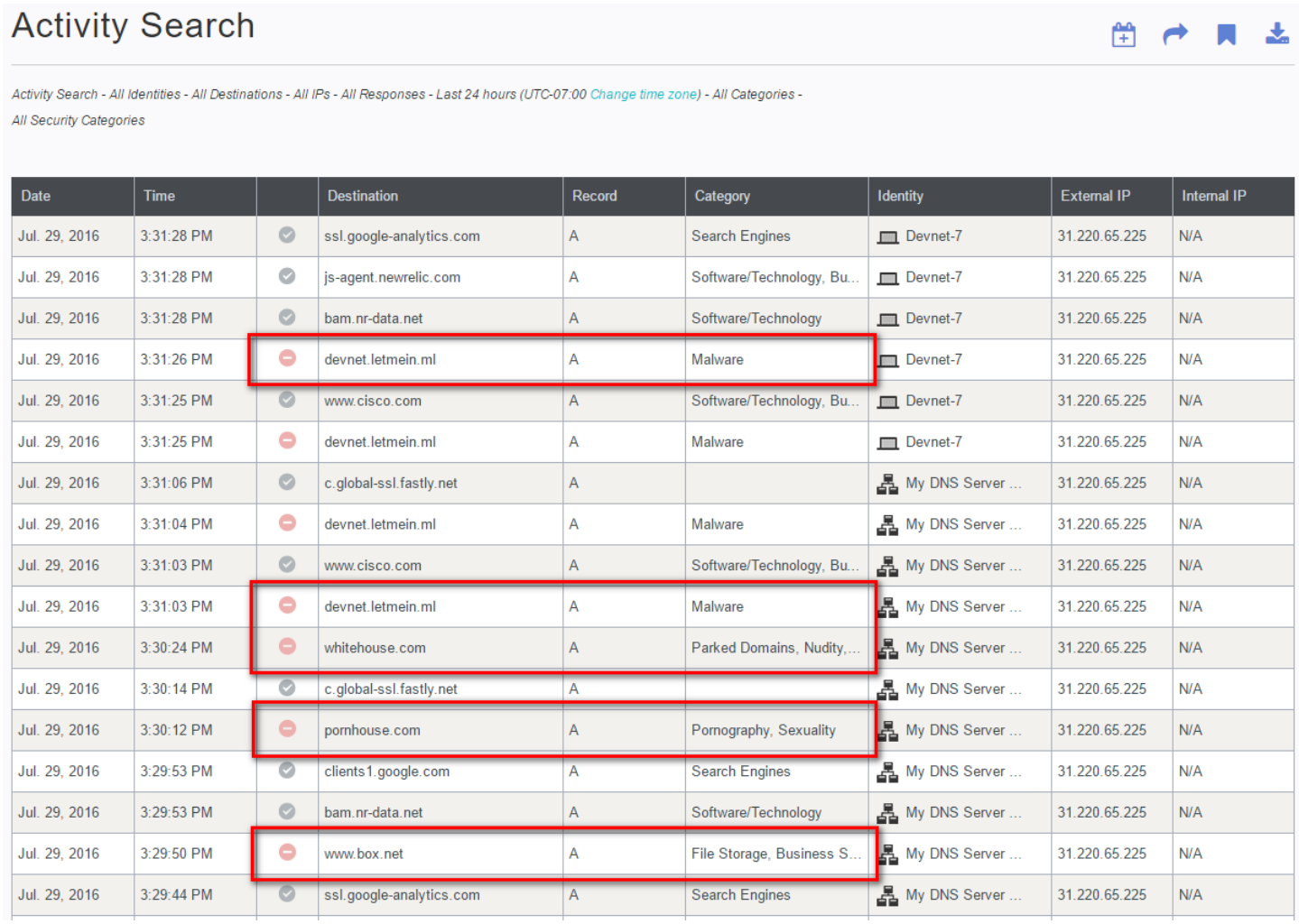
图 35 - 配置新网络



现在，使用内部网络 DNS 服务器的所有系统都已受到保护，所有活动报告也可归因于内部 DNS 服务器发出的请求。

活动报告将显示所有 DNS 查询操作，并明确指定阻止的目的域以及该目的所属的类别。图 36 所示为尝试下载勒索软件或访问其他类别的阻止站点时的阻止域结果。身份信息包括 Umbrella Roaming 客户端系统和来自内部 DNS 服务器的查询。

图 36 - Umbrella 阻止域查询



Activity Search

Activity Search - All Identities - All Destinations - All IPs - All Responses - Last 24 hours (UTC-07:00 Change time zone) - All Categories - All Security Categories

Date	Time		Destination	Record	Category	Identity	External IP	Internal IP
Jul. 29, 2016	3:31:28 PM		ssl.google-analytics.com	A	Search Engines	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:28 PM		js-agent.newrelic.com	A	Software/Technology, Bu...	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:28 PM		bam.nr-data.net	A	Software/Technology	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:26 PM		devnet.letmein.ml	A	Malware	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:25 PM		www.cisco.com	A	Software/Technology, Bu...	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:25 PM		devnet.letmein.ml	A	Malware	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:06 PM		c.global-ssl.fastly.net	A		My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:31:04 PM		devnet.letmein.ml	A	Malware	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:31:03 PM		www.cisco.com	A	Software/Technology, Bu...	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:31:03 PM		devnet.letmein.ml	A	Malware	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:30:24 PM		whitehouse.com	A	Parked Domains, Nudity,...	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:30:14 PM		c.global-ssl.fastly.net	A		My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:30:12 PM		pornhouse.com	A	Pornography, Sexuality	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:29:53 PM		clients1.google.com	A	Search Engines	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:29:53 PM		bam.nr-data.net	A	Software/Technology	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:29:50 PM		www.box.net	A	File Storage, Business S...	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:29:44 PM		ssl.google-analytics.com	A	Search Engines	My DNS Server ...	31.220.65.225	N/A

面向终端的思科高级恶意软件防护 (AMP)

AMP 是一种基于云的“软件即服务”解决方案。当您设置帐户后，您需要配置策略，然后在终端上部署 AMP 轻型连接器。支持的终端包括适用于 Windows、Mac、Linux 和 Android 系统的连接器。如果组织有较高的隐私限制，备用的部署选项包括本地气隙式 AMP 私有云虚拟设备，但该产品不在本解决方案验证的范围之内。

首次登录 FireAMP 控制台时，系统将显示首次使用向导。此向导可以指导您通过一系列步骤快速配置 FireAMP 环境：创建防病毒产品例外项、设置代理、配置策略以及创建组。这些步骤的介绍请参阅《快速入门指南》[4]，此处不再重复。

为了尽可能提供最有效的勒索软件防御，还需完成以下额外的配置步骤。有几项设置将在系统组使用的策略中执行，其他设置则在 AMP 帐户设置中配置。首先，编辑策略设置；根据组织的系统性能和可接受的风险级别适当配置相应的执行模式（主动模式阻止文件运行，直到其散列值分析完毕）。接下来，根据组织的具体情况，加大最大扫描和存档文件大小限制。

> 警告：与默认的“被动”设置相比，将执行模式配置为“主动”可能会对系统性能产生重大影响，特别是对网络连接缓慢或时断时续的系统和/或使用自定义或非主流应用的系统更是如此。系统必须检查每个文件后才会允许其运行（或者判定超时）。

在我们为解决方案验证收集的 1600 多份勒索软件样本中，有 103 份大于“保护策略”中默认的 5MB 最大扫描文件大小（最大者达到 51MB）。

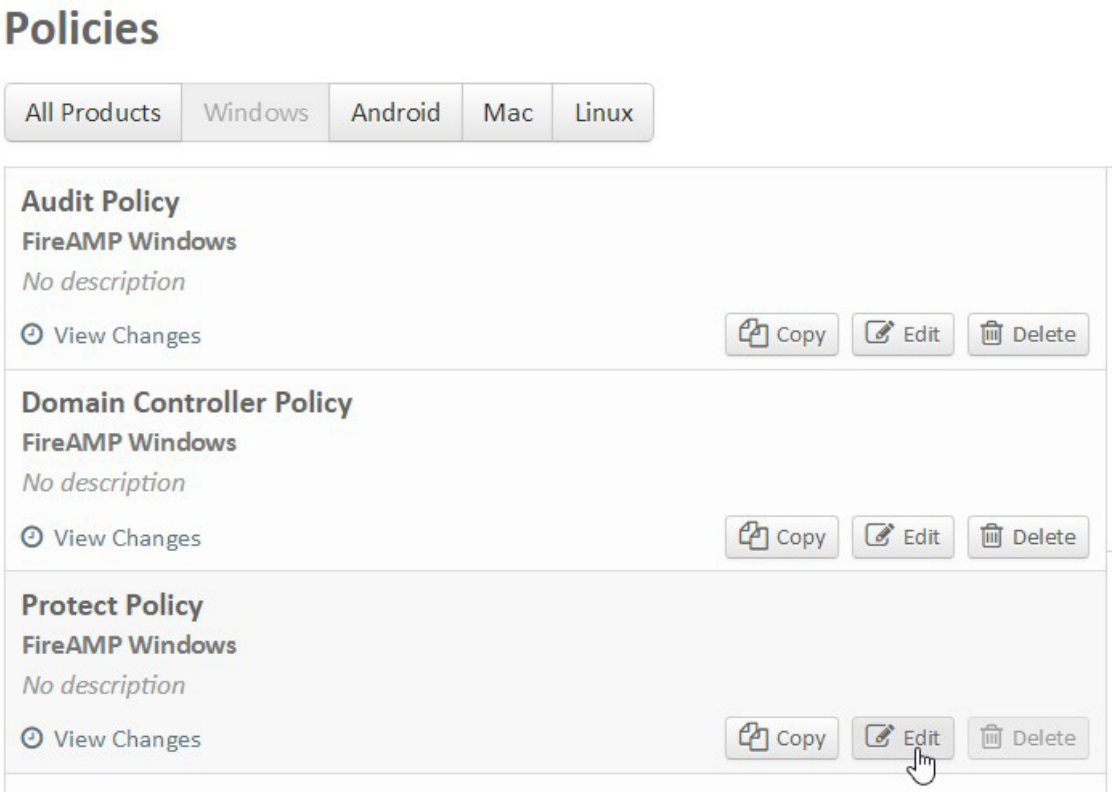
> 注意：如果要扫描的文件大小比较大，会增加到互联网的广域网利用率，并有可能影响其他通信。对于规模较大的组织而言，现场扫描设备可能是首选。

步骤 1 登录 AMP 控制台后，依次选择“管理”>“策略”。

[4] https://docs.amp.cisco.com/FireAMPQuickStartGuide.pdf

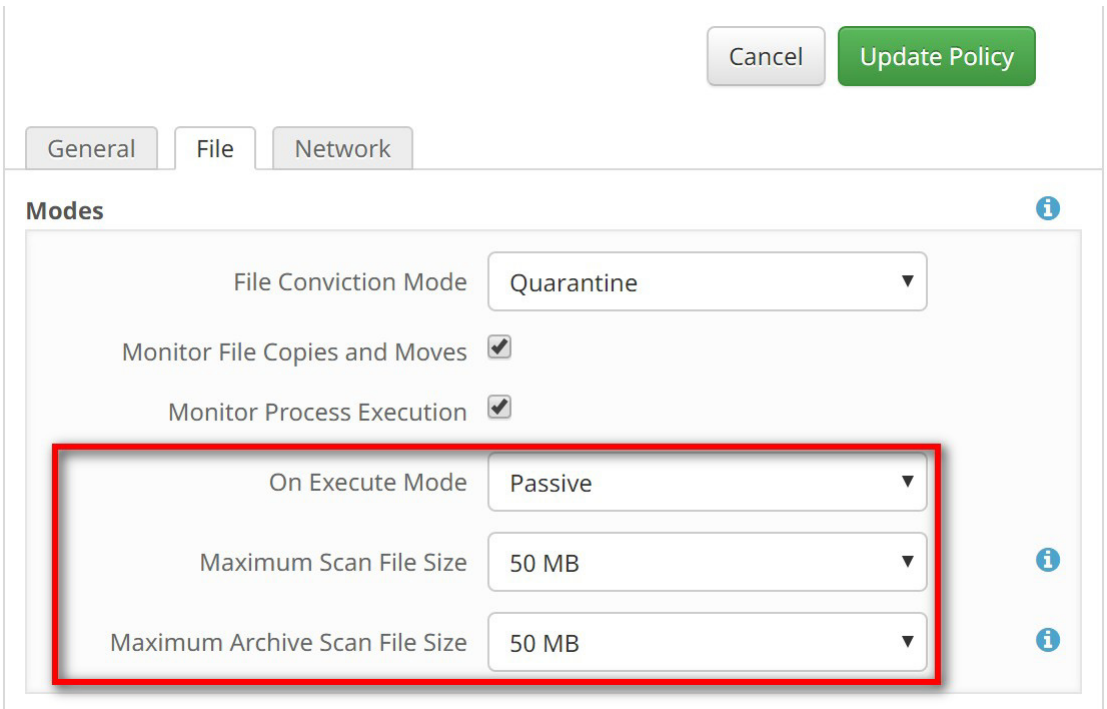
步骤 2 选择您准备部署到终端的相应“保护策略”，然后点击“编辑”。

图 37 - AMP 保护策略



步骤 3 切换到该策略的“文件”选项卡，检查执行模式，并设置最大文件大小。

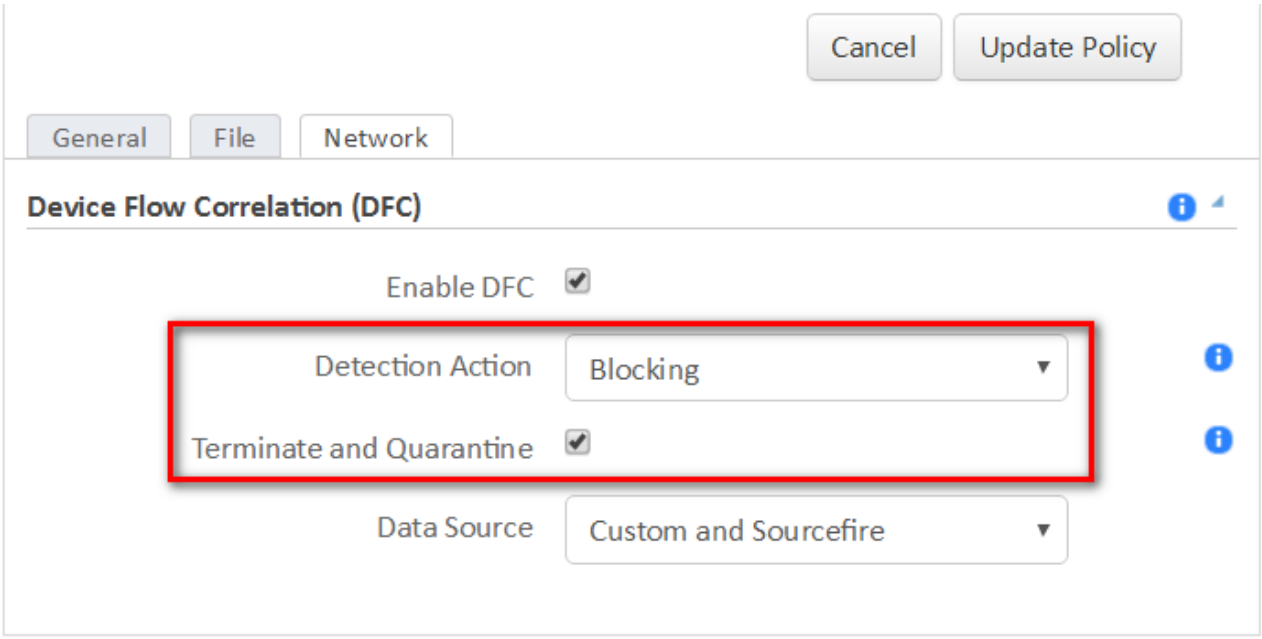
图 38 - 编辑策略的“文件”属性



设备流关联 (DFC) 可以在源头阻止勒索软件回调通信，对公司网络外的远程终端特别有用。

步骤 4 选择“网络”选项卡，将 DFC 操作设置为“阻止”，并选中“终止并隔离”。

图 39 - 编辑策略的“网络”属性



警告！在启用此功能之前，请确保您已将您环境中所有允许的应用列入白名单，特别是所有专有或自定义软件。

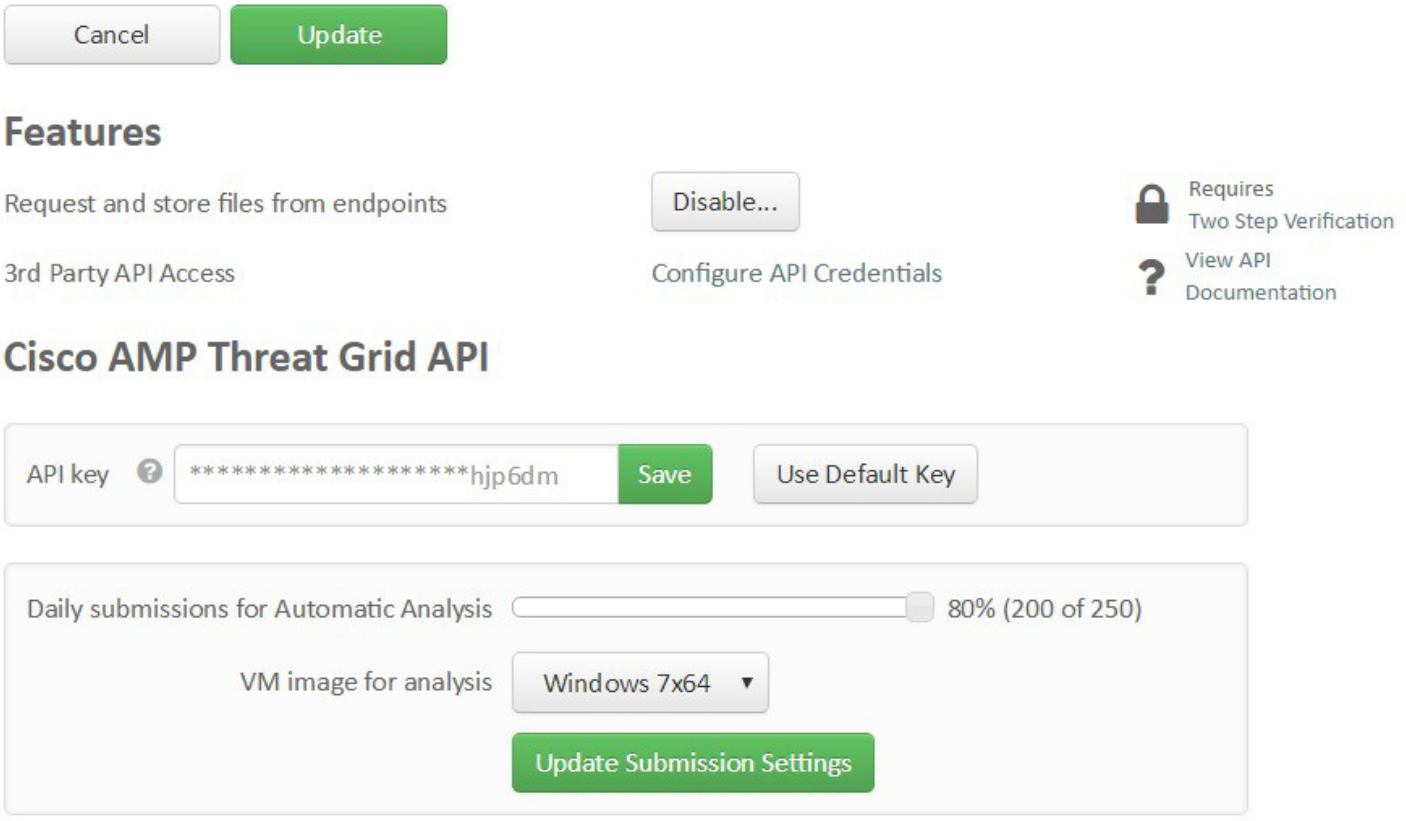
步骤 5 完成后，点击“更新策略”。

思科 AMP Threat Grid API 可用于自动提交文件进行分析。在配置自动分析之前，必须为所有用户的帐户启用双因素身份验证，以确保维持最高级别的隐私，因为分析的所有文件可由控制台中配置的管理用户访问。对帐户启用两步验证后，您就可以编辑帐户的业务设置来启用文件存储库、API 密钥和提交设置。

步骤 6 依次选择“帐户”>“业务”>“编辑”。

步骤 7 在“功能”下，启用“请求并存储来自终端的文件”，设置 Threat Grid API 密钥（如果您有单独的帐户），将“自动分析的每天提交量”滑动到所需程度，并选择最符合您的大多数终端的虚拟机映像。然后点击“更新提交设置”。

图 40 - AMP 帐户的业务设置



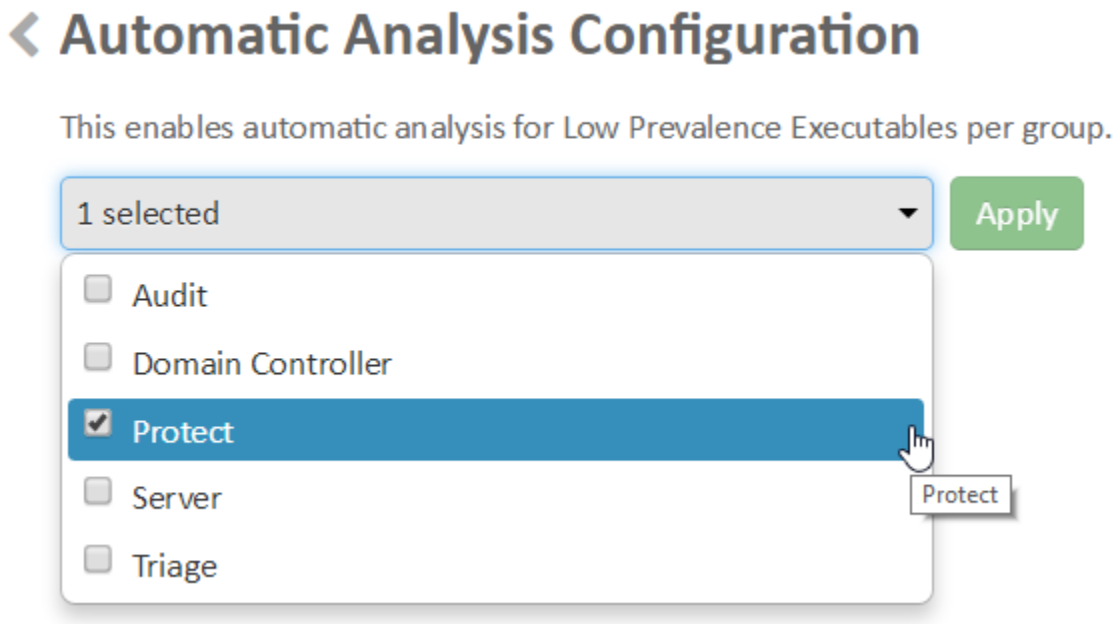
步骤 8 完成后，点击顶部的“更新”以更新帐户设置。

现在，启用自动分析，以便将低普遍性可执行文件从特定的组发送到文件分析功能。

步骤 9 依次选择“分析”>“普遍性”>“配置自动分析”。

步骤 10 选择要为其启用自动分析的系统组，然后点击“应用”。

图 41 - 启用 AMP 自动分析



一旦您配置了自动分析，低普遍性可执行文件会每隔四个小时提交一次。FireAMP 会向观察文件是否可用的 FireAMP 连接器请求文件。检索到文件后，系统会将文件提交至文件分析功能。然后，您可以从“文件分析”页面查看分析的结果。如果在一段时间内未检索到文件，您可以在“文件存储库”中检查文件获取状态。

验证测试

本设计第一阶段的解决方案验证测试将通过以下方法完成：创建一个具有代表性的企业网络，由 Windows 服务器和客户端工作站组成，并能提供全面的互联网连接。测试将实施思科云邮件安全、DNS 安全（通过 Umbrella 实现）和面向终端的 AMP 产品。

在测试勒索软件样本之前，需要先部署服务器和工作站并将其加入 Active Directory 域。然后，配置从工作站到文件服务器的文件共享并映射到盘符。接下来，为邮件服务器部署 Microsoft Exchange，并为用户创建邮件帐户（对部署的每个工作站具有唯一性）。最后，在系统上安装最能代表表 4 中指定的几代典型的基础设施部署和维护版本的各种软件包。

表 4 - 测试系统软件安装

测试系统软件安装版本：							
	XPsp3x86	Win7sp1x64 Enterprise	Win10x64 Enterprise	2008R2 LOW-FS	2012R2 HIGH-FS	2012R2 AD	2012R2 Exchange
Java	Jre-6u45	Jre-7u80	Jre-8u91				
Microsoft Office	2007	2013	2016				
Firefox	5	20	47				
MS IE	8	10	11	8	11	11	11
Acrobat Reader	10	11	DC				
Adobe Flash	12	18	21				
MS .net	2	3.5	4.5	3.5	3.5+4.5		3.5+4.5
MS Silverlight	3	4	5.1				
C++	9.0.3	9.0.3	9.0.3				
主机防火墙	关闭	关闭	关闭	关闭	关闭	关闭	关闭
DNS 到 AD	有	有	有	有	有	有	有
加入 AD	有	有	有	有	有	有	有
静态 IP 和网关	有	有	有	有	有	有	有

21 个系列的勒索软件样本在这些系统上运行，确定了有关以下各项的基线：感染每个系统内部版本的勒索软件、是否需要管理用户权限，以及为本地和网络共享完成加密的速度有多快。在加密系统前执行 DNS 查询无需任何能正常运行的勒索软件样本。我们认为，这是因为使用的已知样本的 C2 域已经关闭或转移，故这些样本无法在基线系统上正常工作，所以我们将其从进一步测试中删除。

由于所有测试样本均从 Threat Grid 文件分析存储库获取，因此当连接器算出文件的 SHA-256 散列值并进行检查时，AMP 立即识别出这些文件。为了创建用于测试的独有勒索软件版本，我们使用重新计算散列值的实用程序修改可执行文件并插入无伤大雅的空格或注释，在不影响勒索软件样本操作能力的情况下更改得出的文件散列值。如此才得以在所有产品中测试低普遍性文件的自动文件分析功能。

总结

勒索软件是一个必将继续发展并影响更多组织的问题。感染攻击一旦得逞，将对组织产生严重的负面业务影响。

本解决方案可以实现确保组织正常运行的目标，让您因为只有极小的可能性会丧失关键系统控制权和受到要挟而高枕无忧。

使用思科勒索软件解决方案时，从新的恶意攻击活动开始到根据威胁情报提供保护的时间为 30 分钟到 4 个小时，显著低于行业平均时间 - 100 天 [5]。

思科勒索软件防御侧重于尽量防御、快速检测和快速遏制，以便在勒索软件攻击突破防线的情况下减少影响。

有关思科勒索软件防御解决方案和产品的详细信息，请访问 www.cisco.com/go/ransomware。

[5] http://www.cisco.com/c/m/en_us/offers/sc04/2016-annual-security-report/index.html?KeyCode=001031927

参考资料

思科 SAFE 简化安全解决方案：
www.cisco.com/go/safe

思科云邮件安全：
http://www.cisco.com/web/products/security/cloud_email/index.html
思科邮件安全：http://www.cisco.com/c/en/us/products/security/email-security/index.html
思科邮件 URL 内容过滤最佳实践：
http://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118775-technote-esa-00.html
IG- teocv

思科 IOS 安全：
https://www.opendns.com/enterprise-security/threat-enforcement/
思科 Umbrella Roaming 客户端安装：
http://info.umbrella.com/rs/opendns/images/TD-Umbrella-Mobility-Roaming-Client-Guide.pdf
DNS 最佳实践
http://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html
为 Windows Server 2012 和 2012 R2 设置 DNS 转发：
https://support.opendns.com/entries/47071344-Windows-Server-2012-and-2012-R2

面向终端的思科高级恶意软件防护：
http://www.cisco.com/c/en/us/products/security/fireamp-endpoints/index.html
思科高级恶意软件保护：
http://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html

思科 Talos - 全面的威胁情报：
http://www.cisco.com/c/en/us/products/security/talos.html
思科 ThreatGrid：
http://www.cisco.com/c/en/us/solutions/enterprise-networks/amp-threat-grid/index.html

思科网络安全：http://www.cisco.com/c/en/us/products/security/web-security/index.html

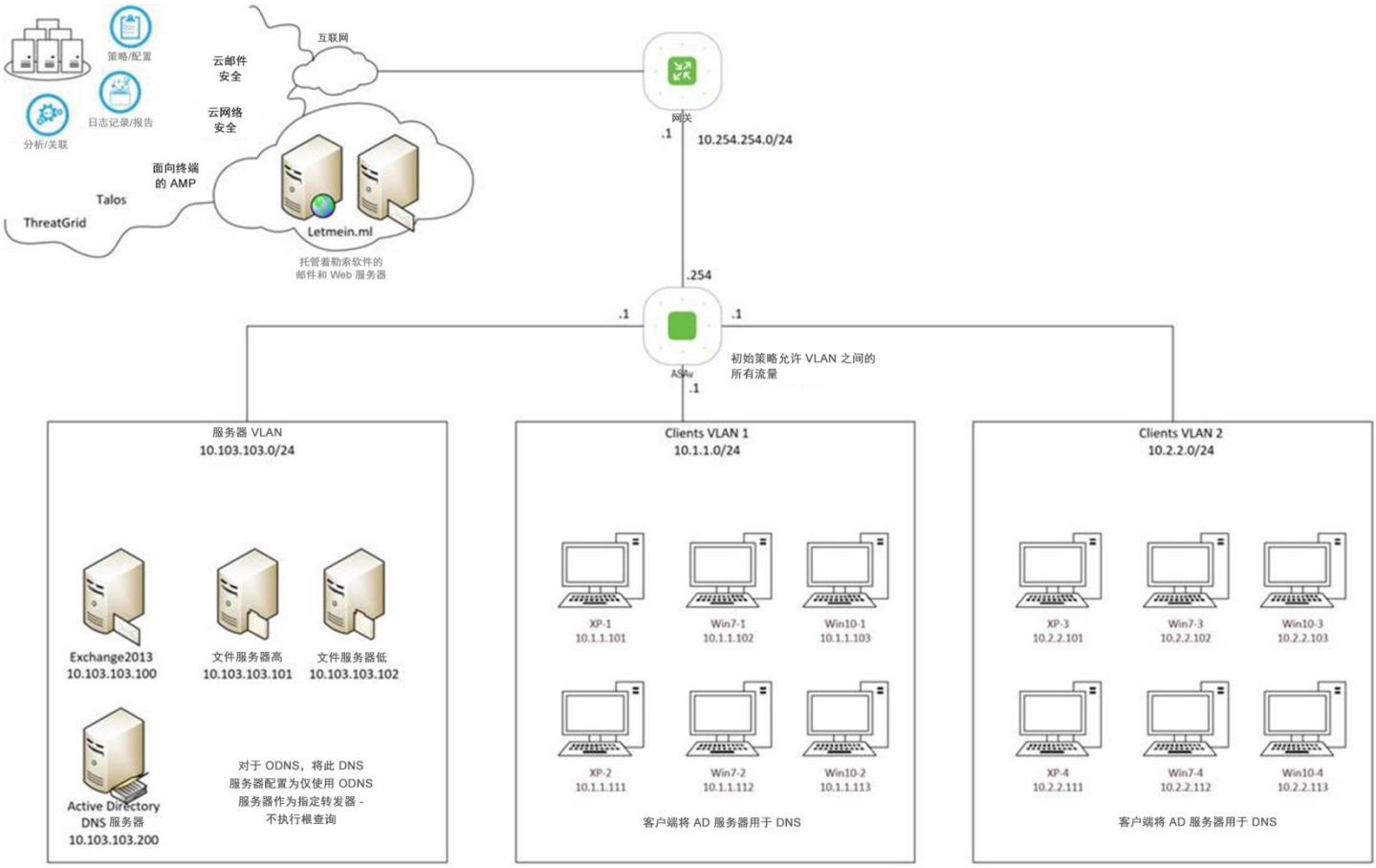
网络即传感器：
http://www.cisco.com/c/en/us/solutions/enterprise-networks/enterprise-network-security/net-sensor.html
思科 Stealthwatch：
http://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
采用 TrustSec 的思科身份服务引擎（网络即执行器）：
http://www.cisco.com/c/en/us/solutions/enterprise-networks/enterprise-network-security/net-enforcer.html
思科快速遏制威胁解决方案：
http://www.cisco.com/c/en/us/solutions/enterprise-networks/rapid-threat-containment/index.html

思科 Firepower 管理中心：
http://www.cisco.com/c/en/us/products/security/firesight-management-center/index.html

附录 A

实验室示意图

图 42 - 实验室示意图



有关 SAFE 的详细信息，请参阅 www.cisco.com/go/SAFE。

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。 地址、电话号码和传真号码均列在思科网站 **www.cisco.com/go/offices** 中。