FireSIGHT 系统版本说明

版本 5.4.0.5 和版本 5.4.1.4

首次发行日期：2015 年 11 月 16 日

最后更新日期：2016 年 8 月 29 日

即使您熟悉更新过程，也请务必通读并理解这些版本说明。这些版本说明描述了受支持的平台、新增功能和更改的功能、已知问题和已解决的问题，以及产品和网络浏览器的兼容性。它们还包含有关以下设备的先决条件、警告以及具体安装说明的详细信息：

- 系列 3 防御中心（DC750、DC1500、DC2000、DC3500 和 DC4000）
- 系列 2 和系列 3 受管设备（3D500、3D1000、3D2000、3D7010、3D7020、3D7030、3D7050、3D7110、3D7115、3D7120、3D7125、3D8120、3D8130、3D8140、3D8250、3D8260、3D8270、3D8290、3D8350、3D8360、3D8370、3D8390、AMP7150、AMP8050、AMP8150、AMP8350、AMP8360、AMP8370 和 AMP8390）
- 具备 FirePOWER 服务的 Cisco ASA（ ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X、ASA5525-X、ASA5545-X、ASA5555-X、ASA5585-X-SSP-10、ASA5585-X-SSP-20、ASA5585-X-SSP-40、ASA5585-X-SSP-60 和 ISA 3000）
- 适用于 Blue Coat X 系列的 Cisco NGIPS
- 64 位虚拟防御中心和受管设备

说明：您无法将运行 FireSIGHT 系统版本 5.3.0.x 的适用于 Blue Coat X 系列的 Cisco NGIPS 直接更新为版本 5.4。必须先卸载旧版本，再安装版本 5.4。请注意，这样会导致有关 X-系列安装的所有配置和事件数据丢失。有关详细信息，请参阅《*用于 X-系列的 FireSIGHT 软件安装和配置指南*》。

提示：有关 FireSIGHT 系统的详细信息，请参阅联机帮助或从支持站点下载《*FireSIGHT 系统用户指南*》。

这些版本说明适用于版本 5.4.0.5 和版本 5.4.1.4 的 FireSIGHT 系统。您可以将物理和虚拟受管设备更新至版本 5.4.0.5。您可以将 Cisco ASA FirePOWER 模块、物理防御中心和虚拟防御中心更新至版本 5.4.1.4。请注意您可以采用以下方式更新设备：

- 防御中心（DC750、DC1500、DC2000、DC3500 和 DC4000）必须运行版本 5.4，才能更新至版本 5.4.1.4。如果您的防御中心目前运行的是更早的版本，您必须先将其更新至版本 5.4，再更新至版本 5.4.1.4。

  说明：防御中心可以在运行版本 5.4 的时候更新设备，但是如果您的防御中心仍然为版本 5.4，您将无法解密或检测 SSL 流量。如果您计划解密或检测 SSL 流量，请将您的防御中心更新至版本 5.4.1.4。

- 系列 2 设备（3D500、3D1000、3D2000、3D2100、3D2500、3D3500、3D4500、3D6500）必须运行版本 5.4，才能更新至版本 5.4.0.5。如果您的系列 2 目前运行的是更早的版本，您必须先将其更新至版本 5.4，再更新至版本 5.4.0.5。
- 系列 3 设备（3D7010、3D7020、3D7030、3D7050、3D7110、3D7115, 3D7120、3D7125、3D8120、3D8130、3D8140、3D8250、3D8260、3D8270、3D8290、3D8350、3D8360、3D8370、3D8390、AMP7150、AMP8050、AMP8150、AMP8350、AMP8360、AMP8370 和 AMP8390）必须运行版本 5.4，才能更新至版本 5.4.0.5。如果您的系列 3 目前运行的是更早的版本，您必须先将其更新至版本 5.4，再更新至版本 5.4.0.5。

- ASA FirePOWER 模块（ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X、ASA5585-X-SSP-10、ASA5585-X-SSP-20、ASA5585-X-SSP-40 和 ASA5585-X-SSP-60）设备必须运行版本 5.4，才能更新至版本 5.4.0.5。如果您的 ASA FirePOWER 模块运行的是更早的版本，您必须先将其更新至版本 5.4，再更新至版本 5.4.0.5。ASA FirePOWER 模块（ASA5506-X、ASA5506W-X、ASA5506H-X、ASA5508-X、ASA5516-X、以及 ISA 3000）必须运行至少版本 5.4.1，才能更新为版本 5.4.1.4。有关部署和安装模块的详细信息，请参阅《*Cisco ASA FirePOWER 模块快速入门指南*》。

有关详细信息，请参阅以下各节：

新功能

本版本说明中，该节汇总了在版本 5.4.0.5 和版本 5.4.1.4 中的 FireSIGHT 系统中新增和更新的特性与功能：

有关详细信息，请参阅《*FireSIGHT 系统用户指南*》、《*FireSIGHT 系统安装指南*》、《*FireSIGHT 系统虚拟安装指南*》和《*适用于 Blue Coat X 系列的 Cisco NGIPS 安装和配置指南*》。

术语

在参阅版本 5.3 1.x 或 5.3.0.x 的相应文档时，可能会注意到这些文档中使用的术语与 版本 5.4.0.5 和版本 5.4.1.4 文档中的术语有所不同。

表 1　　术语更改

版本 5.4.0.5 和版本 5.4.1.4 中使用的术语	说明
Cisco	原称为 *Sourcefire*
FireSIGHT 系统	以前是 *Sourcefire 3D 系统*
防御中心 FireSIGHT 防御中心 Cisco FireSIGHT 管理中心	先前为 *Sourcefire 防御中心*
设备 受管设备	以前是 *Sourcefire 受管设备*
适用于 Blue Coat X 系列的 Cisco NGIPS	原称为*用于 X 系列的 Sourcefire 软件*
FireSIGHT 受管设备	是指 FireSIGHT 防御中心管理的所有设备（受管设备和 ASA 设备）

表 1　　术语更改 （续）

版本 5.4.0.5 和版本 5.4.1.4 中使用的术语	说明
Cisco 自适应安全设备 (ASA) ASA 设备	是指 Cisco ASA 硬件
具备 FirePOWER 服务的 Cisco ASA	是指安装了 ASA FirePOWER 模块的 ASA 设备
ASA FirePOWER 模块	是指安装在兼容 ASA 设备上的硬件和软件模块
ASA 软件	是指安装在思科 ASA 设备上的基本软件
自适应安全设备管理 (ASDM)	指用于管理 ASA 功能的自适应安全设备管理器
直接管理	指使用 ASDM 管理 ASA5506-X 上的 ASA FirePOWER 模块
集中管理	指使用 FireSIGHT 管理 ASA5506-X 上的 ASA FirePOWER 模块防御中心

提示：Cisco 文档中可能会将防御中心称为 FireSIGHT 管理中心。防御中心和 FireSIGHT 管理中心是同一设备。

更改的功能

版本 5.4.0.5 和版本 5.4.1.4 中对以下功能做出了更改：

- VLAN 标签现在限制为 0 到 4095 之间的整数。
- 现在，系统支持根据所有端口值匹配 SSL 流量，包括 32768 及更大的值。
- 如果系统检测到一个 URL，但无法对先前查找结果中请求的 URL 进行分类，则系统会尝试使用第二种 URL 查找方法。使用第二种 URL 查找方法时，如果系统不能在两秒内完成 URL 分类，则将该 URL 归为**未分类**类别，并处理该 URL。

早期版本中引入的特性与功能

版本 5.4.1.1

专用 AMP 设备

版本 5.4 中引入了一个新的系列 3 FirePOWER具有额外处理能力的受管设备，旨在使 FireSIGHT 系统的 AMP 功能达到最优化。AMP8050 属于 81xx 系列设备，支持 Netmods，并提供用作专用 AMP 设备所需的额外存储空间。AMP8350 属于 83xx 系列设备，同样支持 Netmods 及 AMP 功能所需的额外存储。AMP8350 型号可用作堆叠单元，分别与 AMP8360、AMP8370 和 AMP8390 搭配使用，形成 2、3、4 个堆栈。

版本 5.4.1:

FirePOWER 服务管理功能

使用 FirePOWER 服务对 Cisco ASA5506-X 进行集中管理

防御中心现在能够采用与管理所有其它 ASA5500-X 设备一样的方式，管理运行于 ASA5506-X 设备上的 FirePOWER 服务（ASA FirePOWER 设备）实施。只要 ASA 平台运行的是版本 9.3.2.2 或更高版本，且 ASA FirePOWER 设备运行的是版本 5.4.1 或更高版本，就可以在一个防御中心中对多个运行 ASA FirePOWER 的 ASA5506-X 设备进行管理。管理员可以配置入侵检测和预防策略、高级恶意软件防护、应用控制、用户和组控制、文件控制以及 URL 过滤，并同时将这些配置运用于多个 ASA5506-X 设备。此外，防御中心可在单一视图中提供关键控制面板、事件视图、警报功能和您的所有 ASA FirePOWER 设备上的报告。

通过 FirePOWER 服务直接管理 Cisco ASA5506-X

Cisco 的自适应安全设备管理器 (ASDM) 可用于执行上述 ASA FirePOWER 的管理功能，但一次只能在一个 ASA5506-X 设备上操作。此外，您可以直接对系统策略、许可和备份与恢复进行管理。

具备 FirePOWER 服务的 Cisco ASA 的管理限制

当前，Cisco ASA FirePOWER 产品包含两款紧密集成的不同产品：ASA 防火墙和 FirePOWER 下一代入侵防御系统 (NGIPS)。虽然已经在两者之间实现关键数据共享，但统一管理平台仍在开发中。

为此，Cisco ASA 功能目前通过 Cisco Security Manager (CSM) 或自适应安全设备管理器 (ASDM) 进行管理，FirePOWER 服务功能通过 Cisco 防御中心进行管理。因此，防御中心不支持以下中的任何一项功能：

- Cisco ASA 基于硬件的功能，包括集群、堆叠、交换、路由、虚拟专用网络 (VPN) 和网络地址转换 (NAT)。
- 配置 ASA 接口。此外，如果是在 SPAN 端口模式下部署 FirePOWER 服务，任何已配置的 ASA 接口都不会显示。
- 关闭、重新启动或管理 ASA 进程。
- 从 ASA 设备创建或恢复备份。
- 编写访问控制规则，以便通过 VLAN 标记条件进行流量匹配。

说明：ASA 平台可提供上述功能，并可通过 ASA 命令行界面 (CLI) 和自适应安全设备管理器 (ASDM) 对其进行配置。有关详细信息，请参阅 ASA FirePOWER 模块文档。

平台改进

VMware 工具支持

您现在可以在 FireSIGHT 系统虚拟设备上使用 VMware 工具。这样可增强与 VMware 环境的兼容性，并可通过启用软关机、迁移和其他特定的虚拟功能来改善对虚拟设备的管理。以下设备可支持 VMware 工具：

- 64 位虚拟防御中心
- 64 位虚拟受管设备

说明：FireSIGHT 系统版本 5.4 或更高版本都可支持 ESXi 版本 5.1 和 ESXi 版本 5.5。

支持 VMware 虚拟设备的 VMXNET3 接口

虚拟设备现在可支持 VMXNET3 接口类型。因此，您可使用高达 10 Gbits/s 的高速网络接口。

多个管理接口

现在您可以在系列 3 防御中心、FirePOWER（系列 3）受管设备和虚拟防御中心上使用多个管理接口端口。您可以设置将一个接口用于管理流量，另一个接口用于事件流量。这样可以改善某些环境中的部署选项。

系列 3 支持

版本 5.4 中引入了 3D7050，该设备是一个 70xx 子系列设备，配有双核四线程处理器、8 GB RAM 和 80 GB 的硬盘驱动器。

LACP 支持

FirePOWER (系列 3) 设备现在可以参与链路汇聚控制协议 (LACP) (IEEE 802.3ad) 协商，将多个链路聚合为一个链路，从而实现链路冗余和带宽共享。

防御中心 2000 (DC2000)

DC2000 是一个新型防御中心设备平台，其性能和容量为 DC1500 的两倍。

防御中心 4000 (DC4000)

DC4000 是一个新型防御中心设备平台，其性能和容量为 DC3500 的两倍。

提高国际兼容性

Unicode 支持

现在系统可以显示通过文件检测、恶意软件检测和 FireAMP 文件事件检测到的文件名。并且，包括双字节编码的字符在内的非西文字符也可显示。

关联规则中的地理位置和安全情报数据

经过更新后，关联规则引擎可以提供连接、地理位置和安全情报数据。您可以根据这两项新的约束条件生成关联事件，或采取关联操作。例如，如果检测到某个特定国家出现了一个 `Impact 1` 入侵事件，您可以设置一个警报，将该信息记录到外部系统日志服务器上。

支持 FireAMP 私有云

在版本 5.4 中，您可以不再使用思科公共云，而使用 FireAMP 私有云。但需要先安装私有云虚拟设备。由于私有云可协调与公共云之间的交互，因此您可以从公共云中获取收集的威胁信息，避免让您网络中的信息处于风险之中。

版本 5.4 中更新了以下特性和功能：

增强型检测和安全功能

集成式 SSL 解密

FirePOWER (系列 3) 设备现在可以在应用攻击、应用和恶意软件检测之前识别 SSL 通信，并解密流量。您可以在任何受支持的系列 3 设备部署模式中使用 SSL 解密，包括内联和被动模式。SSL 策略控制在企业内部使用的 SSL 的特征，并利用 SSL 规则对加密流量的记录和处理进行精细控制。

简化了规范化和预处理程序配置

现在您可以在访问控制策略（而非入侵策略）中配置流量规范化和预处理。这样可以简化配置，尤其是对于新用户而言。敏感数据预处理程序、规则状态、警告和事件阈值仍可在单个入侵策略级别进行配置。

Snort 规则语言中新增 file_type 关键字

Snort 规则语言中新增 **file_type** 关键字，可指定文件类型进行检测。此方法可替代现有的 **flowbits** 驱动方法，并且更为简化。

FireAMP 连接器提供扩展 IoC 支持

FireAMP 现在可提供由数据驱动的动态危害表现 (IoC) 列表。随着提供新的 IoC，防御中心将自动对其提供支持。这样可以增强 IoC 在任何使用了 FireAMP 的部署中的关联能力。

受保护的规则内容

Snort 规则语言新增了一项可在高度安全的环境中使用的功能。现在您可以使用散列数据创建 Snort 内容匹配。如此一来，规则编写者可以指定要搜索的内容，但又绝对不会以明文形式暴露内容。

先前更改的功能

版本 5.4.1.2 中引入了如下功能：

- 您必须在配置堆栈和集群之前，将同一访问控制策略应用于计划用于堆栈或集群的所有设备。
- 现在您可以选择在应用策略期间不进行流量检测，以此防止网络中断。
- 系统不再向 Health Policy 页面报告发现事件状态。
- 现在您可以参照用于阻拦所有带 ::/0 的 IPv6 地址的访问控制规则网络条件集，或用于阻拦所有带 0.0.0.0/0 的 IPv4 地址的网络规则集，创建访问控制策略。
- 现在，当 CPU 使用率从高水平变为正常时，系统会报告一个有关所有 CPU 报告的事件。

版本 5.4.1.1 中引入了如下功能：

- 现在当您上传入侵规则或安装入侵规则更新时，系统会解除所有入侵策略锁定。

版本 5.4.1. 中引入了如下功能：

- 现在，已注册的 ASA 设备在“设备管理”(Device Management) 页面（**设备 (Devices) > 设备管理 (Device Management)**）下的“高级”(Advanced) 选项卡中提供可配置高级选项。
- 现在可以在 ASA 设备上使用 CLI 命令：**show users**。
- 现在，在“警报” (Alerts) 页面下的“高级恶意软件防护警报” (Advanced Malware Protections Alerts) 选项卡中，您仅可以配置对追溯事件或基于网络的恶意软件事件的警报。

版本 5.4 中更新了以下特性和功能：

- 现在您可以在事件查看器（**分析 (Analysis) > 连接 (Connections) > 事件 (Events)**）中查看连接事件的 VLAN 标记。
- 现在系统可识别通过 FTP、HTTP 和 MDNS 协议进行的登录尝试。
- 现在您可以从发现事件中单独选择已存档的连接事件，用于传输至 eStreamer 客户端。
- 运行状况策略中不再包括发现事件的运行状况监控 (Discovery Event Health Monitor)。
- 现在您可以在版本 5.4 中的“事件视图设置” (Event View Settings) 选项卡（**管理员 (Admin) > 用户偏好 (User Preferences) > 事件视图设置 (Event View Settings)**）中，配置先前在版本 4.10.x 中提供的“扩展数据包视图” (Expand Packet View)。
- 现在以 **.rtf** 文件导入自定义入侵规则会生成**效的规则文件“rtf_rule.rtf”：必须是纯文本文件，这是一个 ASCII 或 UTF-8 编码**警告。
- 现在您可以在“入侵事件图” (Intrusion Event Graphs) 页面（**概述 (Overview) > 摘要 (Summary) > 入侵事件图表 (Intrusion Event Graphs)**）生成以下入侵事件性能图表：
  - 在 TCP 流量/数据包中规范化的 ECN 标志
  - 在 TCP 流量/会话中规范化的 ECN 标记
  - ICMPv4 回显规范化
  - ICMPv6 回显规范化
  - IPv4 DF 标记规范化
  - IPv4 选项规范化
  - IPv4 保留标记规范化
  - IPv4 调整大小规范化
  - IPv4 TOS 规范化
  - IPv4 TTL 规范化
  - IPv6 TTL 规范化
  - IPv6 选项规范化
  - TCP 报头填充规范化
  - 无选项 TCP 规范化
  - TCP NS 标记规范化

  - TCP 选项规范化
  - 规范化阻止的 TCP 数据包
  - TCP 保留标记规范化
  - TCP 分段重组规范化
  - TCP SYN 选项规范化
  - 总 TCP 过滤的数据包
  - TCP 时间戳 ECR 规范化
  - 总 UDP 过滤的数据包
  - TCP 紧急旗标规范化
- 现在，您可以在配置显示列的时候，在“连接事件” (Connection Event) 和“安全情报事件” (Security Intelligence Events) 表视图中配置 **HTTP Referrer** 和**用户代理 (User Agent)** 字段。
- 现在您可以在“访问控制策略” (Access Control Policy) 页面 **(策略 (Policies) > 访问控制 (Access Control))** 查看与您的访问控制策略单个规则相关联的警告。在访问控制策略编辑器中，请将您的鼠标指针悬停在规则名称旁边的警告图标上方，并阅读工具提示文本中的警告，或者通过选择页面顶部**显示警告 (Show Warnings)** 按钮查看与您的访问控制策略中引用的所有规则相关联的警告。
- 在版本 5.4 中，当您在启用**内联模式 (Inline Mode)** 的情况下创建网络分析策略时，内联规范化会自动启用。在早期版本中，您必须在内联入侵策略中手动启用内联规范化。请注意从版本 5.3.x 更新至版本 5.4 不会更改您的内联规范化设置。
- 现在您可以添加访问控制规则端口条件，这些条件指定了**协议 (Protocol)** 下拉列表中不包含的未分配协议号。
- 您无需再在访问控制策略中利用辅助规则控制 FTP 数据通道。
- 新的**解压缩 SWF 文件 (LZMA) (Decompress SWF File [LZMA])**、**解压缩 SWF 文件（缩小）(Decompress SWF File [Deflate])** 和**解压缩 PDF 文件（默认）HTTP (Decompress PDF File [Default] HTTP)** 检查预处理程序选项可为 PDF 和 SWF 文件内容提供增强的解压支持。
- TCP 数据流预处理程序现已增强了对 SMTP、POP3 和 IMAP 的协议感知。
- 系统现在提升了对应用流量信息的检测，包括对 DNS 流量中应用数据的检测和其他协议中的用户检测。
- 现在您可以通过配置 LDAP 身份验证，使用通用访问卡 (CAC) 将该卡与用户名关联，这样用户可以使用该访问卡直接登录到系统。
- 系统现在提供增强的 GPRS 隧道协议 (GTP) 支持。

文档更新

您可以从支持站点下载所有更新的文档。在版本 5.4.0.5 和版本 5.4.1.4 中，以下文档进行了更新，以反映新增功能和经过更改的功能，并解决报告的文档问题：

- *FireSIGHT 系统联机帮助*
- *FireSIGHT 系统联机帮助 (SEU)*
- *FireSIGHT 系统用户指南*
- *FireSIGHT 系统安装指南*
- *适用于 Blue Coat X 系列的 Cisco NGIPS 安装和配置指南*

配合版本 5.4.0.5 和版本 5.4.1.4 而更新的文档包含以下错误：

- 《*FireSIGHT 系统用户指南*》中包含如下错误的表述：您可以**使用LAN 上串行 (SOL) 连接上的默认 (eth0) 管理接口上的无人值守管理 (LOM) 对系列 3 设备进行远程监控或管理**。当前不支持将同一 IP 地址同时使用于 LOM 和与您系列 3 设备之间的 SOL 连接。
- 《*FireSIGHT 系统用户指南*》未反映出以下情况：在内存有限的设备上，入侵策略编号可能无法与一个以上的变量集配对。如果您可以应用仅引用一个入侵策略的访问控制策略，则需要验证对入侵策略的每个引用都与同一个变量集配对。将入侵策略与不同的变量集配对会导致占用内存。
- 关于使用用户名“admin”以及在部署设置向导中指定的新管理员帐户密码在 Vmware 控制台登录虚拟设备，《*FireSIGHT 系统虚拟安装指南*》包含如下错误的表述：**如果您没有使用向导更改密码，或者正在使用 ESXi OVF 模板进行部署，请使用“Cisco”作为密码。**正确的表述应该是：如果您没有使用向导更改密码，或者正在使用 ESXi OVF 模板进行部署，请使用 **Sourcefire** 作为密码。(CSCut77002)

准备工作：重要更新和兼容性说明

在开始版本 5.4.0.5 和版本 5.4.1.4 的更新过程之前，您应熟悉更新过程中的系统行为，以及任何兼容性问题或者更新前后需要进行的配置更改。

注意：Cisco **强烈**建议您在维护时间段、或在中断对部署影响最小的时间段执行更新。

有关详细信息，请参阅以下各节：

配置和事件备份准则

在您开始更新之前，Cisco 强烈建议删除或移动设备上的所有备份文件，然后将当前的事件和配置数据备份到外部位置。

使用防御中心备份自己及其管理的设备的事件和配置数据。有关备份和恢复功能的详细信息，请参阅《*FireSIGHT 系统用户指南*》。

说明：防御中心会清除来自以前的更新的本地存储备份。要保留存档的备份，请将备份存储到外部。

注意：必须在您的 DC2000 和 DC4000 设备上运行 BOIS 版本 2.0.1b，才能更新至版本 5.4.0.5。如果由于 BIOS 版本不兼容导致设备更新失败，请联系支持部门。

更新期间的流量和检查

更新过程会重启受管设备。取决于设备的配置和部署方式，以下功能会受到影响：

- 流量检查，包括应用感知和控制、URL 过滤、安全情报、入侵检测和防御以及连接日志记录
- 流量，包括交换、路由、NAT、VPN 及相关功能
- 链路状态

请注意，当您更新集群设备时，系统会每次更新一台设备，以避免流量中断。

流量检查和链路状态

在内联部署中，受管设备（取决于型号）可通过应用控制、用户控制、URL 过滤、安全情报和入侵防御，以及交换、路由、NAT 和 VPN 来影响流量。有关设备功能的详细信息，请参阅*《FireSIGHT 系统安装指南》*。

下表提供了有关流量、检查和链路状态在更新时会受到何种影响（取决于部署）的详细信息。请注意，无论您如何配置任何内联集，在更新过程中都**不会**执行交换、路由、NAT 和 VPN。

表 2　　网络流量中断

部署	网络流量是否被中断？
带有可配置旁路的内联 （内联集启用了**可配置旁路**选项）	网络流量会在更新过程中的两个时间点发生中断： ■ 更新过程开始时，在链路关闭和打开（摆动），以及网卡切换到硬件旁路时，流量会短暂中断。硬件旁路期间不会检查流量。 ■ 更新完成后，在链路摆动以及网卡退出旁路时，流量会再次短暂中断。端点重新连接，并与传感器接口重新建立链路后，将会再次检查流量。 虚拟设备、适用于 Blue Coat X 系列的 Cisco NGIPS、具备 FirePOWER 服务的 Cisco ASA、8000 系列上的非旁路网络模块或 71xx 系列设备上的 SFP 收发器**不**支持可配置旁路选项。
线内	在整个更新过程中，网络流量会被阻止。
被动	在更新过程中，网络流量不会中断，但也不会对其进行检查。

交换和路由

系列 3 设备在更新过程中**不**会执行交换、路由、NAT、VPN 或相关功能。如果您将设备配置为仅执行交换和路由，则网络流量在更新过程中会被阻止。

更新过程中的审计日志记录

在更新具有网络界面的设备时，系统完成其更新前任务之后，简化的更新界面页面将会显示。直到更新过程完成和设备重新启动之后，对设备的登录尝试才会反映在审核日志中。

更新为版本 5.4.0.5 和版本 5.4.1.4 的版本要求

要更新至版本 5.4.1.4，防御中心必须至少运行版本 5.4。运行版本 5.4.1.1 的防御中心可以管理运行版本 5.4.0.5 和版本 5.4.1.4 的设备。如果运行的是较低版本，可从支持站点获取更新。

防御中心必须运行至少版本 5.4，才能将其受管设备更新至版本 5.4.1.4。

设备或 ASA 模块的当前版本与发行版本（版本 5.4.0.5 或版本 5.4.1.4）越接近，更新所需的时间就越少。

注意：必须在您的 DC2000 和 DC4000 设备上运行 BOIS 版本 2.0.1b，才能将设备更新至版本 5.4.0.5 或版本 5.4.1.4。如果由于您的 DC2000 和 DC4000 运行的 BIOS 版本过低而导致设备更新失败，请联系支持部门。

更新为版本 5.4.0.5 和版本 5.4.1.4 的时间和磁盘空间要求

下表提供了版本 5.4.0.5 和版本 5.4.1.4 更新的磁盘空间和时间指导原则。请注意，使用防御中心更新受管设备时，防御中心需要其 **/Volume** 分区有额外的磁盘空间。

注意：在更新过程中的任何时候都**不**得重新开始更新或重启设备。Cisco提供的时间预估仅供参考，实际更新时间因设备型号、部署和配置而异。请注意，在更新的预先检查部分和重启后，系统可能会呈非活动状态；这是预期的行为。

更新的重新启动部分包括数据库检查。如果在数据库检查过程中发现错误，更新需要更长时间才能完成。与数据库交互的系统后台守护程序，在数据库检查和修复期间不会运行。

如果遇到更新进度方面的问题，请联系支持部门。

表 3　　时间和磁盘空间要求

设备	/上的空间	/Volume 上的空间	管理器中的 /Volume 上的空间	Time
系列 3 受管设备	225 MB	10891 MB	1705 MB	108 分钟
系列 3 防御中心	300 MB	7782 MB	n/a	136 分钟
适用于 Blue Coat X 系列的 Cisco NGIPS	4919 MB	`/mnt/aplocaldisk` 上 54 MB	1089 MB	40 分钟
虚拟防御中心	306 MB	5742 MB	n/a	123 硬件相关
虚拟受管设备	304 MB	5295 MB	1422 MB	因硬件而异
ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X、ASA5585-X-SSP-10、ASA5585-X-SSP-20、ASA5585-X-SSP-40 和 ASA5585-X-SSP-60 上的具备 FirePOWER 服务的 Cisco ASA	98 MB	6695 MB	1097 MB	56 分钟
ASA5506-X、ASA5506W-X、ASA5506H-X、ASA5508-X、ASA5516-X 以及 ISA 3000 上的具备 FirePOWER 服务的 Cisco ASA	9 MB	4867 MB	848 MB	150 分钟

更新为版本 5.4.0.5 和版本 5.4.1.4 后的产品兼容性

必须使用版本至少为 5.4.1 版的防御中心来管理运行版本 5.4.1.4 的设备。要管理 ASA5506-X 上的 ASA FirePOWER 模块，ASA5506W-X、ASA5506H-X、ASA5508-X 或 ASA5516-X 设备，您**必须**至少使用 5.4.1 版的防御中心。

表 4　　管理版本要求

设备	要由运行版本 5.4.1.4 的防御中心管理必须达到的最低版本
FirePOWER受管设备	FireSIGHT 系统的版本 5.3
适用于 Blue Coat X 系列的 Cisco NGIPS	FireSIGHT 系统版本 5.3 1
ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X、ASA5585-X-SSP-10、ASA5585-X-SSP-20、ASA5585-X-SSP-40 和 ASA5585-X-SSP-60 上的 具备 FirePOWER 服务的 Cisco ASA	FireSIGHT 系统版本 5.3.1
ASA5506-X、ASA5506W-X、ASA5506H-X、ASA5508-X、ASA5516-X 以及 ISA 3000 上的具备 FirePOWER 服务的 Cisco ASA	FireSIGHT 系统 5.4.1 版本

说明：您无法将运行 FireSIGHT 系统版本 5.3.0.x 的适用于 Blue Coat X 系列的 Cisco NGIPS 直接更新为版本 5.4。必须先卸载旧版本，再安装版本 5.4。请注意，这样会导致有关 X-系列安装的所有配置和事件数据丢失。有关详细信息，请参阅《*适用于 Blue Coat X 系列的 Cisco NGIPS 安装和配置指南*》。

操作系统兼容性

您可以在以下托管环境中托管运行版本 5.4.1.4 的 64 位虚拟设备：

- VMware vSphere 虚拟机监控程序/VMware ESXi 5.1
- VMware vSphere 虚拟机监控程序/VMware ESXi 5.5
- VMware vCloud Director 5.1

您可以在运行版本 9.3.2.2 或更高版本的以下 ASA 平台上安装运行版本 5.4.0.5 的 ASA FirePOWER 模块：

- ASA5512-X
- ASA5515-X
- ASA5525-X
- ASA5545-X
- ASA5555-X
- ASA5585-X-SSP-10、ASA5585-X-SSP-20、ASA5585-X-SSP-40 和 ASA5585-X-SSP-60

您可以在运行版本 9.3.2.2 或更高版本的 ASA5506-X、ASA5506W-X、ASA5506H-X、ASA5508-X、ASA5516-X 以及 ISA 3000 设备上安装运行版本 5.4.1.4 的 ASA FirePOWER 模块。

有关详细信息，请参阅*《FireSIGHT 系统安装指南》*或*《FireSIGHT 系统虚拟安装指南》*。

您可在运行 XOS 版本 9.7.2 及更高版本，以及版本 10.0 及更高版本的 X-系列平台上运行版本 5.4.0.5的适用于 Blue Coat X 系列的 Cisco NGIPS。有关详细信息，请参阅*《适用于 Blue Coat X 系列的 Cisco NGIPS 安装和配置指南》*。

网络浏览器兼容性

用于 FireSIGHT 系统 Web 界面的版本 5.4.0.5 和版本 5.4.1.4 已在下表中列出的浏览器上进行了测试。

说明：如果您使用的是 Microsoft Internet Explorer 11 浏览器，您必须在 Internet Explorer 设置（**工具 (Tools) > Internet 选项 (Internet Options) > 安全 (Security) > 自定义级别 (Custom level)**）中禁用**上传文件至服务器时包括本地目录路径**选项。

表 5　　受支持的网络浏览器

浏览器	需要启用的选项和设置
Chrome 45	JavaScript、Cookie
Firefox 42	JavaScript、Cookie、安全套接字层 (SSL) v3
Microsoft Internet Explorer 9、10 和 11	JavaScript、Cookie、安全套接字层 (SSL) v3、128 位加密、**活动脚本**安全设置、兼容性视图、将**检查存储网页的较新版本**设置为**自动**

屏幕分辨率兼容性

Cisco 建议，至少选择 1280 像素宽的屏幕分辨率。用户界面兼容低分辨率，但高分辨率可优化显示效果。

还原为上一版本

如果您由于某种原因，需要将设备还原为 FireSIGHT 系统的上一版本，请联系支持部门，以便了解详细信息。

重映像设备

如果您因故需要将设备重新映像至当前版本的 FireSIGHT 系统，请参阅《*适用于 Blue Coat X 系列的 Cisco NGIPS 安装和配置指南*》的“安装适用于 Blue Coat X 系列的 Cisco NGIPS”一节（对于适用于 Blue Coat X 系列的 Cisco NGIPS 设备）、《*FireSIGHT 系统虚拟安装指南*》（对于虚拟设备）以及《*FireSIGHT 系统安装指南*》的“将 FireSIGHT 系统设备还原为出厂默认设置”一节（对于所有其他设备）。

请注意，如果卸载某个版本的适用于 Blue Coat X 系列的 Cisco NGIPS，必须重启 VAP 后再安装其它版本。此过程可能需要数分钟。

要从 5.4.1 版映像更新为版本 5.4.0.5 或版本 5.4.1.4，请参阅准备工作：重要更新和兼容性说明，第 8 页和安装更新，第 13 页。

从支持站点下载以下文件：

说明：请直接从支持站点下载映像。如果通过邮件传输映像文件，可能会损坏该文件。

- 对于系列 3 防御中心：

  ```
  Sourcefire_Defense_Center_S3-5.4.0-763-Restore.iso
  ```

- 对于虚拟防御中心：

  ```
  Sourcefire_Defense_Center_Virtual64_VMWare-5.4.0-763.tar.gz
  ```

- 对于系列 2 受管设备：

  ```
  Sourcefire_3D_Device_500-5.4.0-Restore.iso
  Sourcefire_3D_Device_1000-5.4.0-Restore.iso
  Sourcefire_3D_Device_2000-5.4.0-Restore.iso
  Sourcefire_3D_Device_2100-5.4.0-Restore.iso
  Sourcefire_3D_Device_2500-5.4.0-Restore.iso
  Sourcefire_3D_Device_3500-5.4.0-Restore.iso
  Sourcefire_3D_Device_45100-5.4.0-Restore.iso
  Sourcefire_3D_Device_6500-5.4.0-Restore.iso
  ```

- 对于系列 3 受管设备：

  ```
  Sourcefire_3D_Device_S3-5.4.0-763-Restore.iso
  ```

- 对于虚拟受管设备：

  ```
  Sourcefire_3D_Device_Virtual64_VMWare-5.4.0-763.tar.gz
  ```

- 对于适用于 Blue Coat X 系列的 Cisco NGIPS 设备：

  ```
  SF3DSensor-5.4-763.cbi
  ```

- 对于 ASA FirePOWER 模块：

  ```
  asasfr-sys-5.4.0-763.pkg
  ```

- 对于具备 FirePOWER 服务的 Cisco ASA（ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X ASA5516-X，以及 ISA 3000）：

  ```
  asasfr-5500X-boot-5.4.1-211.img
  asafr-sys-5.4.1-211.pkg
  ```

  说明：要在具备 FirePOWER 服务的 Cisco ASA 上安装 ASA FirePOWER 模块版本 5.4.1.4 映像，请参阅《*Cisco ASA FirePOWER 模块快速入门指南*》，了解有关部署和安装模块的详细信息。

安装更新

在您开始更新之前，必须通读和理解这些版本说明，特别是准备工作：重要更新和兼容性说明，第 8 页。

要将运行至少 5.4.1 版的防御中心更新为版本 5.4.1.4，将运行至少版本 5.4.1 的 ASA FirePOWER 模块（ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5516-X，以及 ISA 3000）更新为版本 5.4.1.4，将运行至少 FireSIGHT 系统版本 5.4 的受管设备和 ASA FirePOWER 模块（ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X、ASA5585-X-SSP-10、ASA5585-X-SSP-20、ASA5585-X-SSP-40 和 ASA5585-X-SSP-60）更新为版本 5.4.0.5，请参阅以下概括的指导和程序：

- 更新防御中心，第 14 页
- 更新受管设备、ASA FirePOWER 模块和适用于 Blue Coat X 系列的 Cisco NGIPS，第 15 页

注意：在更新期间**不要**重启或关闭设备，直至看到登录提示。系统在更新的预先检查部分可能呈非活动状态；这是预期的行为，不需要您重启或关闭设备。

何时执行更新

由于更新过程可能会影响流量检查、流量和链路状态，Cisco **强烈**建议您在维护时段或者在中断对部署影响最小的时间执行更新。

安装方法

使用防御中心的网络界面执行更新。先更新防御中心，然后用它更新其管理的设备。

安装顺序

请先更新您的防御中心，然后在更新其管理的设备。

在成对的防御中心上安装更新

开始更新高可用性对中的一个防御中心时，如果它尚未就绪，另一个防御中心将会变为主防御中心。此外，成对的防御中心将会停止共享配置信息；成对的防御中心在常规同步过程中**不会**接收软件更新。

为确保操作的连续性，请**不要**同时更新成对的防御中心。应先完成辅助防御中心的更新操作步骤，然后再更新主防御中心。

在集群设备上安装更新

在集群设备上安装更新时，系统每次对一台设备执行更新。更新开始时，系统会先将更新应用至辅助设备；辅助设备会进入维护模式，直到所有必须进程均已重新启动，随后辅助设备会再次处理流量。接下来，系统会以相同的过程，将更新应用至主设备。

在堆叠设备上安装更新

在堆叠设备上安装更新时，系统同时进行更新。更新完成后，每台设备都会恢复正常运行。请注意：

- 如果主设备先于所有辅助设备完成更新，在所有设备完成更新之前，堆栈会以受限的混合版本状态运行。
- 如果主设备晚于所有辅助设备完成更新，堆栈会在主设备完成更新后恢复正常运行。

在适用于 Blue Coat X 系列的 Cisco NGIPS上安装更新

更新适用于 Blue Coat X 系列的 Cisco NGIPS 将会重新加载受影响的 VAP。如果用于 X-系列的 FireSIGHT 软件设备是内联部署的，且您在使用多成员 VAP 组，则 Cisco 建议您一次更新一个 VAP。这使得正在更新的 VAP 重新加载时，组内的其他 VAP 能够检查网络流量。

说明：如果您在内联部署中使用单一 VAP 的 VAP 组，重新加载 VAP 会导致网络流量中断。请务必将更新安排在维护时段，或对部署影响最小的时间执行。

安装后

当您在防御中心或受管设备上执行更新后，您**必须**重新应用设备配置和访问控制策略。应用访问控制策略可能会导致流量和处理的短时间暂停，还可能会导致一些数据包未经检查地通过。有关详细信息，请参阅*《FireSIGHT 系统用户指南》*。

您还应执行多个额外的更新后步骤，以确保部署可正常执行。其中包括：

- 验证更新是否已成功
- 确保部署中的所有设备都能够成功通信
- 更新至版本 5.4.1.4的最新补丁（如有），以利用最新的增强功能和安全修复程序
- 或者，更新入侵规则和漏洞数据库 (VDB)，并重新应用访问控制策略
- 根据新功能，第 2 页中的信息进行任何必要的配置更改

以下各节不仅包括有关执行更新的详细说明，还包括有关完成任何更新后步骤的详细说明。确保完成所有列出的任务。

更新防御中心

按照本节所述的操作步骤更新防御中心（包括虚拟防御中心）。对于版本 5.4.1.4 更新，防御中心会重启。

注意：您必须将 DC2000 和 DC4000 BIOs 更新到版本 2.0.1b，才能将您的设备更新为版本 5.4.1.1。从思科支持站点下载 BIOs 更新。

注意：在更新防御中心之前，请将访问控制策略重新应用至所有受管设备。否则，对受管设备的最终更新可能会失败。

注意：在更新期间**不要**重启或关闭设备，直至看到登录提示。系统在更新的预先检查部分可能呈非活动状态；这是预期的行为，不需要您重启或关闭设备。

说明：将防御中心更新为版本 5.4.1.4 会从设备中删除现有的卸载程序。

要更新防御中心，请执行以下操作：

1. 阅读这些版本说明，并完成必要的更新前任务。

   有关详细信息，请参阅准备工作：重要更新和兼容性说明，第 8 页。

2. 从支持站点下载更新：

   - 对于系列 3和虚拟防御中心：

     ```
     Sourcefire_3D_Defense_Center_S3_Upgrade-5.4.1.4-22.sh
     ```

     说明：请直接从支持站点下载更新。如果通过邮件传输更新文件，可能会损坏该文件。

3. 选择 **System > Updates**，然后在 **Product Updates** 选项卡中点击 **Upload Update**，将更新上传到防御中心。浏览到更新并点击 **Upload**。

   更新将会上传到防御中心。网络界面会显示您上传的更新的类型、其版本号以及生成更新的日期和时间。该页面还会指明在更新过程中是否需要重新启动。

4. 确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。

5. 查看任务队列 (**System > Monitoring > Task Status**)，确保没有正在进行的任务。

   必须等到所有长时间运行的任务都完成后，才能开始更新。正在运行的任务会在更新开始时停止，成为失败的任务，并且不能恢复；您必须在更新完成后，将其从任务队列中手动删除。任务队列每 10 秒自动刷新一次。

6. 选择 **System > Updates**。
7. 点击上传的更新旁边的安装图标。
8. 选择防御中心并点击 **Install**。确认要安装更新并重新启动防御中心。

   更新过程将会开始。您可以在任务队列（**系统 [System] > 监控 [Monitoring] > 任务状态 [Task Status]**）中监控更新进度。但是，在防御中心完成其必要的更新前检查后，系统会使您注销。当您重新登录时，系统会显示 Upgrade Status 页面。Upgrade Status 页面会显示进度条，提供当前正在运行的脚本的相关详细信息。

   如果更新由于任何原因而失败，该页面会显示错误消息，其中指明失败的时间和日期、更新失败时正在运行的脚本，并提供有关如何联系支持部门的说明。请**不要**重新开始更新。

   注意：如果更新出现任何其他问题（例如，手动刷新“更新状态”页面后，几分钟都没有显示进度），请**不要**重新开始更新，而应联系支持部门。

   更新完成后，防御中心会显示成功消息，并重新启动。
9. 在更新完成后，应清除浏览器缓存，并强制要求浏览器重新加载。否则，用户界面可能会出现意外行为。
10. 登录至防御中心。
11. 阅读并接受《**最终用户许可协议 (EULA)**》。请注意，如果您不接受 **EULA**，系统会将您从设备注销。
12. 选择 **Help > About**，确认软件版本是否已正确列出：版本 5.4.1.4。另请注意，防御中心上的规则更新和 VDB 的版本；您随后会需要这些信息。
13. 确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。
14. 如果支持站点上的可用规则更新比防御中心上的规则要新，请导入较新的规则。此时请勿自动应用导入的规则。

    有关规则更新的详细信息，请参阅*《FireSIGHT 系统用户指南》*。
15. 如果支持站点上的可用 VDB 比防御中心上的 VDB 要新，请安装最新的 VDB。

    安装 VDB 更新会导致流量和处理的短时间暂停，还可能会导致一些数据包未经检查地通过。有关详细信息，请参阅*《FireSIGHT 系统用户指南》*。
16. 将设备配置重新应用到所有受管设备。

    要重新激活灰显**应用 (Apply)** 按钮，请在设备配置中编辑任意接口，然后在不进行更改的情况下点击**保存 (Save)**。
17. 将访问控制策略重新应用到所有受管设备。

    注意：请**勿**单独重新应用入侵策略；必须完全重新应用所有访问控制策略。

    应用访问控制策略可能会导致流量和处理的短时间暂停，还可能会导致一些数据包未经检查地通过。有关详细信息，请参阅*《FireSIGHT 系统用户指南》*。
18. 如果支持站点提供了版本 5.4.1.4的补丁，请按照该版本的《*FireSIGHT 系统版本说明*》所述，应用最新的补丁。**必须**更新至最新补丁才可利用最新增强功能和安全修复程序。

更新受管设备、ASA FirePOWER 模块和适用于 Blue Coat X 系列的 Cisco NGIPS

在将您的防御中心更新至版本 5.4、版本 5.4.1 或版本 5.4.1.4 后，使用它们来更新其管理的设备。

防御中心必须运行至少版本 5.4，才能将其受管设备更新至版本 5.4.1.4。由于它们没有网络界面，因此必须使用防御中心来更新虚拟受管设备、适用于 Blue Coat X 系列的 Cisco NGIPS 和 ASA FirePOWER 模块。

更新受管设备分两步进行。首先，从支持站点下载更新，并将其上传到管理防御中心。接着，安装软件。可一次对多台设备进行更新，但这些设备必须都使用同一个更新文件。

对于版本 5.4.0.5 更新，所有设备都会重启，而且适用于 Blue Coat X 系列的 Cisco NGIPS VAP 组会重新加载。系列 3 设备在更新过程中**不会**执行流量检查、交换、路由、NAT、VPN 或相关功能。更新过程还可能会影响流量和链路状态，具体取决于设备的配置和部署。有关详细信息，请参阅更新期间的流量和检查，第 8 页。

注意：在更新受管设备之前，请使用其管理防御中心适当的访问控制策略重新应用至受管设备。否则，受管设备的更新可能会失败。

注意：在更新期间**不要**重启或关闭设备，直至看到登录提示。系统在更新的预先检查部分可能呈非活动状态；这是预期的行为，不需要您重启或关闭设备。

提示：如果用于 X-系列的 FireSIGHT 软件是内联部署的，且您在使用多成员 VAP 组，则 Cisco 建议您一次更新一个 VAP。这使得正在更新的 VAP 重新加载时，组内的其他 VAP 能够检查网络流量。如果您在内联部署中使用单一 VAP 的 VAP 组，重新加载 VAP 会导致网络流量中断。请务必将更新安排在维护时段，或对部署影响最小的时间执行。

要更新受管设备和 ASA FirePOWER 模块，以及适用于 Blue Coat X 系列的 Cisco NGIPS：

1. 阅读这些版本说明，并完成必要的更新前任务。

说明：请直接从支持站点下载更新。如果通过邮件传输更新文件，可能会损坏该文件。

有关详细信息，请参阅准备工作：重要更新和兼容性说明，第 8 页。

2. 可以更新设备的管理防御中心上的软件；请参阅更新防御中心，第 14 页。
3. 从支持站点下载更新：
   - 对于系列 2 受管设备：

     `Sourcefire_3D_Device_Upgrade-5.4.0.5-24.sh`

   - 对于系列 3 受管设备：

     `Sourcefire_3D_Device_S3_Upgrade-5.4.0.5-24.sh`

   - 对于或虚拟受管设备：

     `Sourcefire_3D_Device_Virtual64_VMware_Upgrade-5.4.0.5-24.sh`

   - 对于适用于 Blue Coat X 系列的 Cisco NGIPS 设备：

     `Sourcefire_3D_XOS_Device_Upgrade-5.4.0.5-24.sh`

   - 对于 ASA FirePOWER 模块（ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X、ASA5585-X-SSP-10、ASA5585-X-SSP-20、ASA5585-X-SSP-40 和 ASA5585-X-SSP-60）：

     `Cisco_Network_Sensor_Upgrade-5.4.0.5-24.sh`

   - 对于 ASA FirePOWER 模块（ASA5506-X、ASA5506W-X、ASA5506H-X、ASA5508-X、ASA5516-X，以及 ISA 3000）：

     `Cisco_Network_Sensor_Upgrade-5.4.1.4-15.sh`

4. 选择**系统 (System) > 更新 (Updates)**，然后在“产品更新”(Product Updates) 选项卡中点击**上传更新 (Upload Update)**，并将更新上传到防御中心。浏览到更新并点击 **Upload**。

   更新将会上传到防御中心。网络界面会显示您上传的更新的类型、其版本号以及生成更新的日期和时间。该页面还会指明在更新过程中是否需要重新启动。

5. 确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。
6. 点击要安装的更新旁边的安装图标。

7. 选择要安装更新的设备。

   如果要更新堆叠对，选择该对的一个成员，会自动选择另一个成员。您必须同时更新堆叠对中的成员。

8. 点击**安装**。确认要安装更新并重新启动设备。

9. 更新过程将会开始。可在防御中心的任务队列 (**System > Monitoring > Task Status**) 中监控更新进度。

   请注意，在更新过程中，受管设备可能会重新启动两次；这是预期的行为。当 VAP 在内联部署的适用于 Blue Coat X 系列的 Cisco NGIPS 设备上重新加载时，流量中断。

   说明：当您更新 X-系列设备时，必须先等待设备重启，并完全重新加载 VAP 后，再继续其他操作。

   注意：如果更新出现问题（例如，如果任务队列指示更新已失败，或者手动刷新任务队列后，几分钟都没有显示进度），请不要重新开始更新。而应联系支持部门。

10. 选择 **Devices > Device Management**，并确认更新的设备是否具有正确的软件版本：版本 5.4.0.5。

11. 确认部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。

12. 将设备配置重新应用到所有受管设备。

    提示：要重新激活灰显**应用 (Apply)** 按钮，请在设备配置中编辑任意接口，然后在不进行更改的情况下点击**保存 (Save)**。

13. 将访问控制策略重新应用到所有受管设备。

    应用访问控制策略可能会导致流量和处理的短时间暂停，还可能会导致一些数据包未经检查地通过。有关详细信息，请参阅*《FireSIGHT 系统用户指南》*。

14. 如果支持站点提供了版本 5.4.0.5的补丁，请按照该版本的*《FireSIGHT 系统版本说明》*所述，应用最新的补丁。

    必须更新至最新补丁才可利用最新增强功能和安全修复程序。

已解决的问题

您可以使用 Cisco 漏洞搜索工具（https://tools.cisco.com/bugsearch/）跟踪此版本中已解决的漏洞。需要 Cisco 账户。要查看早期版本中解决的缺陷，请参阅传统警告跟踪系统。

版本 5.4.0.5 和版本 5.4.1.4 中已解决的问题：

- **安全问题**解决了以下问题：系统未能正确地将新增的注释编码进访问控制策略中。
- **安全问题**解决了 CVE-2015-4242 中描述的多个跨站请求伪造 (CSRF) 漏洞。
- 解决了以下问题：如果在启用日志记录的情况下创建 SSL 规则，则“连接事件”(Connection Events) 页面不会显示 URL 类别值。(142878/CSCze93434)
- 解决了以下问题：如果以用户身份而非**管理员**身份登录到系统，并对入侵策略的基层进行编辑，则系统将错误地将所有受影响的已编辑入侵策略标记为**管理员**（实际并非管理员）所做的更新。(CSCur79437)
- 解决了以下问题：如果配置一个系统策略，以便使用远程 NTP 服务器将时间同步到连接了注册设备的系统，并禁用设备管理，则在系统启用设备管理后 NTP 无法将已更新的时间同步到设备。(CSCur97671)
- 解决了以下问题：在某些情况下，防御中心会遇到系统问题，导致无法加载访问控制规则。(CSCut30047)
- 解决了以下问题：当系统从 Microsoft Active Directory 服务器下载大量组和用户时，会出现延迟问题，并且系统未能匹配流量至引用 LDAP 组的访问控制规则。(CSCut56233)

- 解决了以下问题：系统错误地处理了带多个接口的系列 3 设备上配置的静态路由。(CSCut84953)
- 解决了以下问题：如果在一个未含有任何发现事件的防御中心上查看“发现数据”(Discovery Statistics) 页面，则系统会显示内部服务器错误。(CSCuu00749)
- 在某些情况下，系统不会生成入侵事件性能图表（**概览 (Overview) > 摘要 (Summary) > 入侵事件性能 (Intrusion Event Performance)**）。(CSCuu15447)
- 解决了以下问题：如果对防御中心进行备份后，在另一个防御中心上恢复备份，则无法登录到已恢复备份的防御中心。(CSCuu35238)
- 解决了以下问题：如果在没有 FireSIGHT 许可证的情况下，下载 LDAP 用户或 LDAP 组到防御中心，则会出现下载失败，并且系统会生成错误提示已达到用户限制。(CSCuu35615)
- 解决了以下问题：在添加或编辑了路由的 IP 地址后，原本并非可配置的思科冗余协议 (SFRP) 广告区间值看似为可配置。(CSCuu37687)
- 解决了以下问题：运行 ASA 最低版本 9.3.2.2 或更高版本的 ASA Firepower 模块未实施 **mpf-policy-map-class** 模式。(CSCuu68273)
- 解决了以下问题：如果在带有集群接口的受管设备上配置静态或虚拟路由器，则系统会错误地禁用已配置的静态路由、虚拟路由器或虚拟路由过滤器。(CSCuu47325)
- 解决了以下问题：如果您创建了一个产品映射并且已选中**添加修复映射 (Add Fix Map)** 选项，系统未能生成供应商列表。(CSCuu79373)
- 解决了以下问题：如果您部署了一条默认动作设置为**解密重签 (Decrypt-Resign)**的 SSL 策略，系统会对从一个接口集发出的解密流量进行交换或路由处理，这样，该流量进入同一受管设备上的不同接口集。(CSCuu97712)
- 解决了以下问题：如果您添加一个以上的许可证至 3D8250 设备并添加一个许可至另一台系列 3 设备，“许可证”(License) 页面错误地在错误设备下列出许可证。(CSCuu99789)
- R解决了以下问题：无法使用 **ucsfg** 思科 UCS 配置实用程序命令进行 DC2000 和 DC4000 BIOS 设置。(CSCuv03352)
- 解决了以下问题：系统在生成的入侵事件中不包含来自 X-Forward-For 和 True-Client-IP 的数据以及其他包数据。(CSCuv03727)
- 解决了以下问题：如果您对受管设备应用了一条未设置为**在内联模式下丢弃 (drop when inline)**的入侵策略，在本该拦截时，系统未能拦截带恶意软件性质的文件。(CSCuv12647)
- 解决了以下问题：如果您启用了两个 IPv6 IP 地址，从“健康监控”(Health Monitor) 页面生成故障排除会失败。(CSCuv27328)
- 解决了以下问题：在配置信誉预处理程序的优先级时，系统未能正确地将**黑名单**作为优先级列表保存，即使您已将信誉服务器配置设置到白名单中。(CSCuv52955)
- 提高了带端口范围的访问控制规则内存的使用率。(CSCuv64114)
- 解决以下问题：如果您修改了主机配置文件的属性设置，在更改主机IP地址后，系统未能保留主机的属性设置。(CSCuv69748)
- 改善了网络映射生成。(CSCuv72386)
- 解决了以下问题：系统未能包括未映射到主机 IP 地址的新用户帐户，并且按用户组检测用户流量的分组访问控制规则失败。(CSCuv78458)
- 解决了以下问题：在系统更新后，您配置的网络分析策略未能正确加载。(CSCuw44448)

早期版本中解决的问题

之前解决的问题按版本列出。

版本 5.4.0.4 和版本 5.4.1.3 中解决的问题：

- **安全问题**解决了 Linux 操作系统中的一个漏洞问题，如 CVE-2011-4131 中所述。
- **安全问题**解决了以下问题：在处理已损坏流量时，受管设备出现了微引擎故障。(CSCuu86214)
- 解决了以下问题：对于单个受管设备，您重应用入侵策略（单个或作为访问控制策略的一部分重新应用）的次数不超过 4096 次。(134385/CSCze89030)
- 解决了以下问题：如果您导入了由另一条策略作为共享或基础策略引用的入侵策略，该入侵策略导入失败。(144946/CSCze96151)
- 解决了以下问题：在入侵策略列表页面，系统两次不正确地列出已注册目标的数量。(CSCus08840)
- 解决了以下问题：即使在事件页面的剪贴板中的事件显示为空，您仍然可以从剪贴板添加旧事件到新事件。(CSCus67128)
- 解决了以下问题：如果您编辑了一条具有多个类别条件的访问控制规则并尝试删除某个条件，系统仅删除第一个列出的类别条件。(CSCut25082)
- 解决了以下问题：如果入侵规则以 8000 系列设备上的被动区为目标并且执行 **show fastpath-rules** CLI 命令，系统报告入侵规则为非活动状态。(CSCut32479)
- 解决了以下问题：在配置文件策略时如果启用**检查存档 (Inspect Archives)** 选项，会导致 Snort 停止传输流量。（CSCut39253、CSCuu60621）
- 改善了故障排除。(CSCut43542)
- 改善了磁盘管理程序的可靠性。(CSCut65740)
- 改善了关联规则性能。(CSCut97938)
- 解决了以下问题：对以 Cisco 开头的 RPM 包管理器文件进行降级处理未能正确的重置 RPM 安装历史记录。(CSCut98525)
- 解决了以下问题：如果您在未编辑访问控制策略的情况下重应用该策略至 ASA FirePOWER 模块，策略应用失败。(CSCuu14839)
- 根据 DCE/RPC 高级设置中重叠端口设置的使用改进了错误消息警告。(CSCuu18577)
- 解决了以下问题：在长时间使用系统之后，至 AMP 云的连接可能会丢失。(CSCuu24587)
- 解决了以下问题：如果您在一个连接到 Cisco Nexus 7000 交换机的物理系列 3设备上创建了一个链路汇聚组 (LAG)，系统会出现流量中断。(CSCuu31626)
- 解决了以下问题：如果您将系统的时区改为 UTC 东部的一个时区并添加一个包含至少一个非活动周期的关联规则至关联策略，策略应用会失败。(CSCuu37600)
- 解决了以下问题：在您的集群系列 3设备上创建路由接口导致连接问题。（CSCuu37668 ）
- 解决了以下问题：如果您生成了一个报告，离开“报告模板”(Report Templates) 选项卡，然后生成另一个报告，**发送电子邮件 (Send email)** 复选框无法保持选定状态。(CSCuu97750)
- 改进了跟踪受监控主机的数量。(CSCuu77263)
- 解决了以下问题：如果您在启用了 IPv6 地址的情况下将防御中心配置为使用静态 IPv4 地址，并使用 IPv6 地址访问防御中心的接口，访问控制策略编辑器页面没有加载。(CSCuu83933)

- 解决了以下问题：在极少数情况下，系统会不稳定，并且无法通过硬复位进行恢复。(CSCuu93154)
- 解决了以下问题：某些 DC4000 设备上的驱动器故障导致 RAID 控制器故障和数据丢失。(CSCuu93159)
- 解决了以下问题：即使存在 URL 过滤许可证，“产品许可”(Product Licensing) 控制面板构件未列出任何 URL 过滤许可证。(CSCuu97762)
- 改善了 SFDatacorrelator 的性能。(CSCuv48373)

版本 5.4.0.3 和版本 5.4.1.2 中解决的问题：

- **安全问题**解决了会使客户端连接遭到外部攻击的多个 SSLv3 漏洞，如 CVE-2015-0286、CVE-2015-0287、CVE-2015-0289、CVE-2015-0292 和 CVE-2015-0293 中所述。
- **安全问题**解决了一个跨站脚本 (XSS) 漏洞，如 CVE-2015-0707 中所述。
- **安全问题**解决了 Linux 和其它第三方操作系统中的多个漏洞问题，如 CVE-2011-2699、CVE-2012-2744、CVE-2012-3400 和 CVE-2015-1781 中所述。
- **安全问题**解决了 HTTP 连接处理漏洞，该漏洞允许用户被重定向到恶意网站，如 CVE-2015-0706 中所述。
- **安全问题**解决了以下问题：基于 Firepower 7000 或 8000 系列受管设备检查的流量中的畸形数据包数据，系统出现了微引擎故障。（CSCuu10871、CSCuu26678）
- 如果路由是系列 3 设备上配置的，系统可以转发源路由 IPv4 数据包，这样会通过不同于在路由器上配置的路径传输数据包，而且可以避开网络安全措施。(132121/CSCze88520)
- 解决了以下问题：如果您从生成的事件查看某些文件的威胁评分，系统会错误地将威胁评分报告为数字，而非**低**、**中**、**高**或**非常高**。(142290/CSCze93722)
- 改进了 URL 过滤。(144198/CSCze94590)
- 解决了以下问题：7000 系列设备的被动接口报告的出口安全区和接口不正确。(144624/CSCze95206)
- 解决了以下问题：如果从“对象管理”页面编辑接口安全区，堆叠设备配置看起来似乎是最新的，但实际上并非如此。(144626/CSCze94847)
- 解决了以下问题：如果您启用远程存储，并在防御中心上创建预定的邮件告警响应，则预定的邮件告警会禁用远程存储，且远程存储备份会失败。(145288/CSCze95993)
- 解决了以下问题：如果网络上的用户在地址栏中输入非小写的 URL，则包含 Web 应用条件的访问控制规则与流量不匹配。(CSCur37364)
- 解决了以下问题：如果将高可用性配置的防御中心添加到系统，会导致辅助防御中心覆盖系统文件列表中现有的 SHA-256 值。(CSCur57708)
- 解决了以下问题：如果创建的关联规则会在发生入侵事件或连接事件，且条件将入口安全区、出口安全区、入口接口或出口接口匹配为条件，则系统无法识别您创建的规则，且无法针对与该规则匹配的流量生成事件。(CSCur59840)
- 增强的多个控制面板构件。(CSCus11068)
- 解决了以下问题：在 Snort 重启过程中，系统有时会出现延迟情况。(CSCus13247)
- 解决了一个漏洞，该漏洞导致采用 uuencode 编码的邮件附件的文件名无法显示在文件事件和恶意软件事件中。(CSCus30831)
- 解决了以下问题：某些 HTTPS 流量检查会导致误报。(CSCus32474)
- 解决了以下问题：如果已注册 ASA FirePOWER 设备的密码包含不受支持的字符，系统会生成**内部服务器错误 (Internal Server Error)** 消息。(CSCus68604)
- 解决了以下问题：系统在用户第二次尝试通过 HTTP 下载可疑文件时才生成恶意软件告警，而不是在用户第一次尝试下载可疑文件时就生成告警。(CSCus83151)

- 解决了以下问题：如果在“用户管理”页面的“自定义用户角色”(Custom User Role) 选项卡中创建用户角色，系统会禁用某些复选框，但会启用被禁用复选框下的某些可用选项。(CSCus87248)
- 解决了以下问题：如果文件下载过程受阻并重新下载文件，则系统无法识别文件类型，或者系统会生成不正确的 SHA256 值。(CSCus87799)
- 如果系统在 VDB 安装后重启或重新加载，且未选中防火墙策略的**在应用策略期间检查流量 (Inspect Traffic During Policy Apply)** 选项，则在重启过程中网络连接可能会断开。(CSCut08225)
- 解决了以下问题：如果创建的访问控制规则被配置为向外部系统日志服务器发送事件，当系统检测到多个截断的统一文件时，设备会停止向系统日志服务器发送连接事件。(CSCut14629)
- 改进了 SFDatacorrelator 在处理历史电子邮件和 eStreamer 警报时性能。(CSCut23688)
- 解决了以下问题：四端口 10Gbps 非旁路网络模块上的 FirePOWER 光纤端口不能可靠地实现与 APCON IntellaFlex 或 IntellaPatch 品牌设备之间的链路连接。(CSCut24654)
- 解决了系统会在网络文件轨迹页面的错误文件类型信息的问题。(CSCut27978)
- 解决了以下问题：在“入侵事件”表视图中启用“原始客户端 IP”列并查看一行或多行时，系统会生成错误。(CSCut41458)
- 解决了以下问题：系统在可通过外壳访问的网络界面以及日志文件的的系统日志消息中显示了明文密码。(CSCut80473)
- 解决了以下问题：“追溯性恶意软件事件”表不包含追溯性恶意软件事件的新旧处置字段。(CSCut83512)
- 解决了以下问题：如果重启配置了大量子接口的 ASA5585-X 设备，但不同时重启 SFR5585-X 服务卡，则 SFR5585-X 服务卡似乎会出现故障。(CSCut89619)
- 解决了以下问题：如果配置的域名不包含 DNS 条目，则网络界面页面不会加载。(CSCut89714)
- 解决了以下问题：如果您在防御中心遇到云连接中断情况时从防御中心删除恶意软件许可证，系统会连续生成如下运行状况监控器告警：**无法连接云 (Cannot connect to cloud)**。(CSCut95470)
- 解决了以下问题：配置 Windows TGM 代理会导致检测预处理器中断。(CSCut95588)
- 禁用多管理器接口配置中的其中一个管理接口不再会禁用通信信道。(CSCut95915)
- 解决了以下问题：如果链路汇聚组 (LAG) 被配置为使用链路汇聚控制协议 (LACP)，当 LAG 接口遇到大量的广播流量时，LAG 接口会进入强制关闭状态。(CSCuu04209)
- 解决了以下问题：如果云连续检查新的更新，系统会出现问题。(CSCuu04844)
- 如果您尝试创建名称相同的两个关联策略，系统会生成告警。(CSCuu14720)
- 解决了以下问题：如果将 ASA5585-X 设备降级为较旧版本，Linux 不会按预期自动降级。(CSCuu14965)
- 解决了以下问题：系统在“系统负载”控制面板构件中显示不正确的内存使用量。(CSCuu19742)
- 改进了系列 3 理设备上适用于简单网络管理协议 (SNMP) 代理的 CPU 性能报告。(CSCuu31029)
- 改进了 CPU 性能。(CSCuu35011)
- 解决了以下问题：运行 ASA 平台版本 9.3(3) 或 9.4(1) 的 ASA5506-X 设备如果遇到问题，会停止处理流量。(CSCuu38535)
- 解决了以下问题：过度使用内存会导致系统重新开始进程，进而可能导致网络连接中断。(CSCuu88135)
- 解决了以下问题：在从“报告”页面生成报告时，如果点击可配置的**中继主机 (Relay Host)** 选项旁边的“编辑”图标，则网络浏览器会重定向到内部服务器错误网页。(CSCuv01286)

版本 5.4.1.1 和版本 5.4.0.2 中解决的问题：

- **安全问题** 解决了会使客户端连接遭到外部攻击的多个 SSLv3 漏洞，如 CVE-2014-3569、CVE-2014-3570、CVE-2014-3572 和 CVE-2015-0204 中所述。
- **安全问题**解决了一个随机脚本注入漏洞，该漏洞使未经身份验证的远程攻击者可以攻击 GNU C 函数库的 DNS 解析功能，如 CVE-2015-0235 中所述。
- **安全问题**解决了多个跨站脚本 (XSS) 漏洞和随机 HTML 注入漏洞。（CSCus03591、CSCus03762、CSCus04436、CSCus07858 和 CSCus07875）
- **安全问题**解决了 通用唯一标识符 (UUID) 处理方面的一个漏洞。(CSCus06097)
- 解决了以下问题：查看规则文档时，如果在入侵规则编辑器中编辑本地规则，系统会对已生成的事件数据显示当前的本地规则配置，而不显示触发这些数据的规则配置。(145118/CSCze95346)
- 解决了以下问题：如果您备份和还原防御中心，系统不会备份或还原安全情报对象。（CSCur42337、CSCur35624）
- 解决了 3 系列受管设备的以下问题：在设备重启过程中，支持旁路的内联集可能会断开内联连接多达 25 秒。(CSCur64678)
- 解决了以下问题：在某些情况下，您无法获得有关 URL 类别或 URL 信誉的信息。（CSCur38971、CSCus59492）
- 解决了以下问题：如果从网络图的“漏洞”选项卡根据客户端应用展开漏洞，系统不会显示关联的主机。(CSCur86191)
- 解决了以下问题：在某些情况下，如果其中一项访问控制规则操作设置为“拦截”(Block) 或“交互拦截”(Interactive Block)，则主机无法始终显示拦截页面。(CSCus06868)
- 解决了以下问题：使用 Windows 文件共享 (SMB) 时，由于报告名称包含不受支持的字符，因此系统不支持生成多种报告类型。(CSCus21871)
- 解决了以下问题：如果将创建的 SSL 策略设置为“不解密”(Do Not Decrypt)，并尝试建立会话，系统会错误地将该会话报告为“已被拦截”，但事实并非如此。(CSCus41127)
- 解决了以下问题：如果将引用文件策略的访问控制规则置于带有 Web 应用条件的访问控制规则后面，且所引用的文件策略带有恶意软件拦截规则，则系统无法识别恶意软件文件。（CSCus64393、CSCus64526）
- 解决了以下问题：如果系统的管理接口和控制接口使用同一个 VLAN，而管理接口使用 IPv6 地址，则管理接口不可用。(CSCus64678)
- 解决了以下问题：如果系统包含 SSL 可见性设备 (SSLVA) 或 Cisco SSL 设备，且您创建包含 Web 应用类别和恶意软件拦截规则的文件策略，则您第一次通过 HTTPS 下载文件时会失败。注意此问题解决，当SSL设备运行的是版本 3.8.4。
- 解决了以下问题：如果应用的访问控制策略引用 URL 过滤许可证、安全情报许可证或配置为用于检查以下任何设备的 SSL 策略，则系统会遇到问题：7000 系列、ASA5506-X、ASA5506H-X 和 ASA5506W-X。(CSCut02823)
- 进一步精简了关联事件表。(CSCut02984)
- 解决了以下问题：如果在启用了“Spero 分析”和“文件捕获”功能的情况下创建文件策略，则系统无法捕获在传入流量中检测到的文件。(CSCut06837)
- 如果应用的访问控制策略具有规则集且使用的都是 IPv4 源地址，则系统会评估使用 IPv6 源地址的流量，就好像规则中没有设置源地址一样。如果应用的访问控制策略具有规则集且使用的都是 IPv6 源地址，则系统会评估使用 IPv4 源地址的流量，就好像规则中没有设置源地址一样。如果应用的访问控制策略具有规则集且使用的都是 IPv4 目标地址，则系统会评估使用 IPv6 目标地址的流量，就好像规则中没有设置目标地址一样。如果应用的访问控制策略具有规则集且使用的都是 IPv6 目标地址，则系统会评估使用 IPv4 目标地址的流量，就好像规则中没有设置目标地址一样。(CSCut48596)
- 解决了以下罕见问题：如果 3 系列设备检测到流向堆叠设备的流量，则系统会遇到问题，无法处理流量。(CSCut53335)

版本 5.4.1 中解决的问题：

- **安全问题**解决了会使客户端连接遭到外部攻击的多个 SSLv3 漏洞。该次修复针对 CVE-2014-3566。
- **安全问题**解决了一个随机脚本注入漏洞，该漏洞使未经身份验证的远程攻击者可以通过 bash 执行命令。该次修复针对 CVE-2014-6271 和 CVE-2014-7169。
- **安全问题**解决了通用唯一标识符 (UUID) 处理方面的未经授权访问漏洞。
- **安全问题**解决了主机属性的跨站脚本 (XSS) 漏洞。
- **安全问题**解决了 HTML 注入漏洞。
- 加快了在应用访问控制策略过程中重新加载 Snort 配置的速度。（112070/CSCze87966、CSCur19687）
- 解决了以下问题：如果在创建的 SSL 策略中，文件“会话未缓存”(Session Not Cached)选项设置为**不解密 (Do Not Decrypt)** 或**拦截 (Block)**，且 SSL 会话重用功能已启用，那么，当会话刷新时，系统会在“连接事件”表视图的 **SSL 状态 (SSL Status)** 列中显示未缓存会话错误。(143335/CSCze93608)
- 解决了以下问题：如果向运行版本 5.4 的防御中心注册运行版本 5.3.X 的设备，则系统无法显示“入侵事件”表视图和“连接事件”表视图的**网络分析策略 (Network Analysis Policy)** 列的数据。(143349/CSCze94484)
- 解决了以下问题：在设备进入维护模式且遇到电源故障的情况下，如果您尝试重启集群系列 3 设备，则系统无法恢复。(143504/CSCze94928)
- 更新了《*FireSIGHT 系统用户指南*》，以反映以下情况：应用访问控制策略可能会导致流量和处理出现短暂中断。(143514/CSCze94971)
- 访问控制策略现在有以下日志记录功能：**在连接开始和结束时进行日志记录**、**在连接结束时进行日志记录**以及**连接时不进行日志记录**。(143507/CSCze94975)
- 解决了以下问题：如果系统生成文件事件，系统会在网络界面的多个页面上错误地截断包含冒号的文件事件文件名。(143666/CSCze94954)
- 解决了以下问题：如果您禁用包含入侵策略或变量集的访问控制规则，而所包含的入侵策略或变量集不同于任何已启用的访问控制规则，那么策略应用会失败，且系统会遇到问题。（143871/CSCze94114、144635/CSCze95200）
- 改进了生成报告时的磁盘管理器清理能力。（143933/CSCze94240、143934/CSCze94286）
- 解决了以下问题：单个主机配置文件无法正确显示多个 IP 地址。(144259/CSCze94623)
- 解决了以下问题：解密的 SSL 会话在连接日志中将 URL 显示为 **http://** 而非 **https://**。(144485/CSCze95739)
- 解决了以下问题：如果创建的自定义网络变量和默认变量具有相同的名称，但两者的名称大写不一样，则系统会误以为自定义变量和默认变量是同一个变量，因此会禁止您删除自定义变量。（144488/CSCze95591、144544/CSCze95599）
- 解决了以下问题：如果您对 DHCP 启用防御中心或受管设备的 **eth1**，则系统会在 **eth0** 和 **eth1** 都启用了 DHCP 的情况下错误地保存配置。(144525/CSCze95666)
- 解决了以下问题：如果在启用了存档文件类型的设备上应用访问控制规则，且该设备运行低于版本 211 的漏洞数据库 (VDB)，则策略应用会失败。(144533/CSCze95570)
- 解决了以下问题：系统将 DNS 流量当作 OpenVPN、QQ 和 Viber 流量来处理。(144548/CSCze95536)
- 解决了以下问题：无法禁用规则或数据包延迟阈值计时器。(144555/CSCze95704)
- 解决了以下问题：如果您在连接到 8000 系列受管设备的网络模块上创建链路汇聚组 (LAG) 接口，然后关闭设备，那么，在关闭设备后删除网络模块会导致错误。(144576/CSCze95166)
- 解决了以下问题：从系统删除 URL 过滤许可证会导致云连接中断。(144578/CSCze95183)

- 解决了以下问题：如果在通过 ASA 会话命令登录的情况下，在 ASA5506-X 设备上使用 SFR **system restart** CLI 命令，则设备会停止进程，且不会重新开始这些进程。(144609/CSCze94873)
- 解决了以下问题：网络浏览器会将您创建的 HTML 报告错误地显示为二进制数据。(144667/CSCze95195)
- 解决了以下问题：无法导入和导出防御中心策略。（144806/CSCze95396、144905/CSCze96093）
- 解决了以下问题：为源端口或目标端口定义大量端口会导致策略应用失败。(144933/CSCze95305)
- 解决了以下问题：系统在更新过程中会遇到 FSIC 故障。(144964/CSCze95780)
- 解决了以下问题：如果您尝试在不使用代理选项的情况下建立私有云连接，即使您取消选中“使用代理”选项，系统仍会尝试通过代理连接私有云。(144968/CSCze95801)
- 解决了以下问题：如果您在管理 X-系列设备时尝试下载更新，则自动更新会失败。(145060/CSCze95372)
- 解决了以下问题：如果您尝试使用**下载更新 (Download Updates)** 按钮来更新系统，则用户界面会提供不准确的补丁版本。(145174/CSCze95284)
- 解决了以下问题：在海拔为 2000 英尺的位置，AMP8150 会发出过大噪音，因为其送风风扇的运行速度为 20,000 RPM 或更快；但报告的风扇转速低至 0 RPM。更新 BMC 固件或应用此更新可解决固件问题；如果要暂时解决问题以便进行更新，请使用 **ipmi mc reset cold** CLI 命令重置 AMP8150 基板管理控制器 (BMC)。请注意，重置后，必须重新建立 LAN 上串行 (SOL) 会话。(CSCus59936)
- 解决了以下问题：在**裁剪数据以适应窗口 (Trim Data to Window)** 选项已启用的情况下，内联规范化预处理器会错误地调整数据包大小。(CSCur80901)

版本 5.4 中解决的问题：

- **安全问题**解决了 Linux 和其它第三方操作系统中的多个漏洞问题，如 CVE-2013-0343、CVE-2013-2164、CVE-2013-2206、CVE-2013-2232、CVE-2013-2234、CVE-2013-2888、CVE-2013-3552、CVE-2013-4387、CVE-2013-4470、CVE-2013-4786、CVE-2007-6750、CVE-2013-7263 和 CVE-2013-7265 中所述。
- **安全问题**解决了多个注入漏洞，包括 HTML 和命令行注入。
- **安全问题**解决了多个跨站脚本 (XSS) 漏洞。
- **安全问题**解决了多个跨站请求伪造 (CSRF) 漏洞。
- **安全问题**解决了多个参数处理和配置错误漏洞。
- 如果访问控制规则配置为**拦截 (Block)**、**拦截并重置 (Block with reset)**、**交互拦截 (Interactive block)**、**交互拦截并重置 (Interactive Block with reset)** 或 **监控 (Monitor)**，则选择信誉级别时会同时选择严重性高于所选级别的所有信誉。如果访问控制规则配置为**允许 (Allow)** 或**信任 (Trust)**，则选择信誉级别时会同时选择严重性低于所选级别的所有信誉。(111747/CSCze87908)
- 系统会阻止您使用 IPv6 地址来配置与用户代理之间的连接。(124377/CSCze88700)
- 解决了以下问题：在某些情况下，系统会在入侵事件性能图表中包含无关的数据。(124934/CSCze87728)
- 改进了 eStreamer 绩效指标的功能。(129840/CSCze89231)
- 解决了以下问题：如果在系统开始修剪之前，磁盘空间使用率超过磁盘空间阈值，则大型系统备份会失败。(132501/CSCze88368)
- 解决了以下问题：使用 RunQuery 工具执行 **SHOW TABLES** 命令会导致查询失败。(132685/CSCze89153)
- 解决了以下问题：在某些情况下，对受管设备执行远程备份会在防御中心上生成大量备份文件。(133040/CSCze89204)
- 您现在可以在受管设备的网络界面中，通过“管理接口”页面（**系统 (System) > 本地 (Local) > 配置 (Configuration) > 管理接口 (Management Interfaces)**)的“接口”(Interface) 选项卡编辑最大传输单位 (MTU)。不再可以从防御中心受管设备编辑管理接口的 MTU(133802/CSCze89748)

- 解决了以下问题：在预处理器选项已启用的情况下，入侵规则针对事件生成的系统日志告警消息会引致 `Snort Alert` 消息而非自定义消息。(134270/CSCze88831)
- 解决了以下问题：如果在启动了**快速端口扫描 (Fast Port Scan)** 和**使用来自事件的端口 (Use Port from Event)** 选项的情况下配置 Nmap 扫描补救措施，则补救措施会失败。(134499/CSCze88810)
- 解决了以下问题：如果在高可用性系统中启用“连接结束”日志记录，而会话提前终止，则系统不会报告会话或报告不正确的时间戳。(134806/CSCze89822)
- 解决了以下问题：防御中心和云之间的通信问题不会生成运行状况告警。(134888/CSCze90122)
- 解决了以下问题：如果从“事件视图设置”页面启用**解析 IP 地址 (Resolve IP Addresses)**，系统不会按预期在控制面板或事件视图中解析与 Ipv6 地址相关联的主机名。(135182/CSCze90155)
- 自定义 HTTP 响应页面现在最多支持 50,000 个纯文本字符。(136295/CSCze90383)
- 解决了以下问题：如果指定之前在运行 Windows 操作系统的计算机上创建的源 URL，系统会在“安全情报”(Security Intelligence) 选项卡的工具提示中显示不正确的已提交 IP 地址数量。(136557/CSCze89888)
- 解决了以下问题：如果禁用受管设备上的物理接口，与该物理接口关联的逻辑接口也会被禁用，但这些逻辑接口在编辑器的“接口”(Interfaces) 选项卡中仍显示为绿色。(136560/CSCze89894)
- 解决了以下问题：如果将访问控制策略应用到多台设备，防御中心会在网络界面的“任务状态”(Task Status) 页面、“访问控制策略”(Access Control Policy) 页面和“设备管理”(Device Management) 页面上显示不同的任务状态。(136614/CSCze89936)
- 解决了以下问题：具有 TCP 协议条件的自定义入侵规则根据 UDP 流量而非 TCP 流量生成事件。(136843/CSCze89941)
- 解决了以下问题：捕获的文件表被错误地列为自定义表库的选项。(136844/CSCze89977)
- 解决了以下问题：系统对 DNP3 预处理器规则 145:1、145:2、145:3、145:4、145:5 和 145:6 生成误报。(137145/CSCze90786)
- 解决了以下问题：如果使用超过 40 个字符的主机名注册受管设备，设备注册会失败。(137235/CSCze90144)
- 解决了以下问题：如果在过滤条件中包括任何以下特殊字符，系统无法正确地在对象管理器中过滤对象：美元符号 ($)、脱字号 (^)、星号 (*)、方括号 ([ ])、竖线 (|)、正斜杠 (\)、句点 (.) 和问号 (?)。(137493/CSCze90413)
- 解决了以下问题：如果在系统策略中启用简单网络管理协议 (SNMP) 轮询，并且在某个集群受管设备上修改接口配置，则系统会生成错误的 SNMP 轮询请求。(137546/CSCze90000)
- 解决了以下问题：在访问控制规则中启用系统日志或简单网络管理协议 (SNMP) 连接日志记录会导致系统问题。(137952/CSCze90538)
- 解决了以下问题：即使未计算出 SHA256 值，文件事件的表视图似乎仍支持按文件名查看文件轨迹。(138155/CSCze90676)
- 解决了以下问题：如果生成 HTML 或 PDF 格式的报告，且该报告包含与 x 轴**文件名**相同的图表，则系统不会在 x 轴中显示 UTF-8 字符。(138297/CSCze90799)
- 解决了以下问题：在极少数情况下，修改和重新应用入侵策略几百次会导致入侵规则更新和系统更新需要超过 24 小时才能完成。(138333/CSCze90747)
- 解决了以下问题：如果尝试将地理位置数据库 (GeoDB) 更新为防御中心上已安装的版本，则系统会生成错误消息。(138348/CSCze90813)
- 解决了以下问题：记录到外部系统日志或简单网络管理协议 (SNMP) 陷阱服务器的连接事件的 **URL 信誉 (URL Reputation)** 值不正确。(138504/CSCze91066)

- 解决了以下问题：如果在部署中应用多个访问控制策略，并搜索与特定访问控制规则匹配的入侵或连接事件，会检索到其他策略中不相关的规则生成的事件。(138542/CSCze91690)
- 解决了以下问题：似乎支持剪切并粘贴访问控制规则。(138713/CSCze91012)
- 解决了以下问题：如果防御中心运行的是版本 5.3，eStreamer 运行的也是版本 5.3，则防御中心上的安全情报事件会错误地混淆目标 IP 值和源 IP 值。(138740/CSCze91402)
- 解决了以下问题：如果将设置为**内联模式下丢弃 (drop when inline)**的入侵策略应用到具有被动接口的设备，则系统不会生成有关被忽略的内联规范化设置的警告。(139177/CSCze91163)
- 解决了以下问题：在极少数情况下，“任务状态”页面会将失败的系统策略错误地报告为已成功应用。(139428/CSCze92142)
- 解决了以下问题：系统不会在系列 2 备或虚拟设备上执行最大传输单位 (MTU) 设置。(139620/CSCze91705)
- 解决了以下问题：如果配置并保存通过其基本策略彼此引用的三个或更多的入侵策略，系统不会更新“入侵策略”页面上策略的**上次修改 (Last Modified)** 日期。(139647/CSCze91353)
- 解决了以下问题：如果配置并保存一份报告，该报告带有一个包含从使用夏令时 (DST) 过渡到不使用 DST 的过渡日的时段，系统会将该时段调整为比指定时间提前 1 小时开始。(139713/CSCze91697)
- 解决了以下问题：如果在受管设备的虚拟路由器之间交换接口，则系统不会激活交换接口的休眠静态路由。(139929/CSCze91619)
- 解决了以下问题：如果未向防御中心注册设备，且防御中心没有数据，那么，查看“入侵事件图表”页面（**概述 [Overview] > 摘要 [Summary] > 入侵事件图表 [Intrusion Event Graphs]**）会导致出现以下错误：**警告：由于不是内联模式，规范化被禁用**。(140117/CSCze92324)
- 解决了以下问题：系统允许在外部经过身份验证的用户使用 FireSIGHT 系统网络界面修改密码。(140143/CSCze91938)
- 解决了以下问题：无法一次就成功导入自定义 HTTPS 证书。(140283/CSCze92162)
- 解决了以下问题：在“安排”页面（**系统 [System] > 工具 [Tools] > 安排 [Scheduling]**）上新建任务会导致系统显示授权错误消息。(140575/CSCze92225)
- 解决了以下问题：旁路模式显示为集群设备的一个选项，即使该选项无法启用。(140604/CSCze92047)
- 解决了以下问题：以条形图形式创建的报告最多显示 10 天。(140833/CSCze92405)
- 解决了以下问题：如果用户密码已过期，“用户管理”页面上的**密码生存期 (Password Lifetime)**列会显示负值。(140839/CSCze92338)
- 解决了以下问题：如果禁用引用入侵策略的访问控制规则，然后重新应用访问控制规则，则系统会错误地指出设备的入侵策略已过时。(141044/CSCze92012)
- 解决了以下问题：无法删除第三方漏洞。(141103/CSCze92621)
- 解决了以下问题：系统故意不存储的文件连同**失败的文件存储 (Failed File Storage)** 值错误地显示在事件查看器和控制面板中。(141196/CSCze92629)
- 解决了以下问题：系统提供的保存的搜索 **Public Addresses Only** 包含 172.16.0.0/12 私有 IP 地址范围。(141285/CSCze92654)
- 解决了以下问题：如果将防御中心更新为版本 5.4，该更新会覆盖对“连接摘要”控制面板（**概述 [Overview] > 控制面板 [Dashboards] > 连接摘要 [Connection Summary]**）所做的任何更改。(141363/CSCze92812)
- 解决了以下问题：报告不会为 IP 地址解析主机名。(141393/CSCze92797)
- 解决了以下问题：如果在访问控制策略中启用了 **HTTP 拦截响应 (HTTP Block Response)**，当 Web 服务器的工作主机达到其打开连接极限时，HTTP 拦截响应会导致会话保持打开状态以及 Web 服务器超时。(141440/CSCze92753)

- 解决了以下问题：保存太多次入侵策略修订会导致系统性能问题。(141501/CSCze92792)
- 解决了以下问题：3D9900 设备的安全区外的被动接口不会生成入侵事件和连接事件。(141663/CSCze93022)
- 现在，只需从操作菜单选择**将此规则设置为在所有本地创建的策略中生成事件 (Set this rule to generate events in all locally created policies)** 选项，便可从所生成事件的数据包视图启用规则。(142058/CSCze93416)
- 解决了以下问题：在极少数情况下，系列 3 设备会遇到延迟。(142110/CSCze93561)
- 解决了以下问题：如果防御中心文件发送到云以在沙盒环境中执行动态分析，而云在 50 分钟内不可用，则文件状态会保持为**已发送供分析 (Sent for Analysis)** 而非超时状态。(142309/CSCze93757)
- 解决了以下问题：如果防御中心错误地分配无效的串行信头，则防御中心无法成功地将事件发送到 eStreamer 客户端。(143201/CSCze93686)
- 解决了以下问题：如果在“按应用列出的拒绝连接”控制面板构件中点击某个应用，系统不会正常地将得出的事件视图限制为被阻止的连接。(143376/CSCze93645)
- 解决了以下问题：如果只以 CSV 格式生成一个报告，报告查询将忽略“继承时间窗”(Inherit Time Window) 选项。(143403/CSCze94376)
- 解决了以下问题：如果系统出现丢包情况，则 Modbus 预处理程序无法生成事件。(142450/CSCze95921)
- 解决了以下问题：如果您创建了一条引用设置为解密流量的 SSL 策略的访问控制策略，策略应用会失败。(144518/CSCze94864)
- 解决了以下问题：如果您创建了一条入侵策略或网络分析策略并将共享层加入该策略，然后导出并导入新策略，系统生成**“后端导入失败”(Back-end failed for import)** 错误，并且不会导入策略。(144905/CSCze96093)

已知问题

以下已知问题在版本 5.4.0.5 和版本 5.4.1.4 中有报告：

- 在某些情况下，如果您的 RAID 控制器设置为节能模式，系统可能会生成无关的运行状况警报。(142214/CSCze87267)
- 在某些情况下，内存使用率运行状况监控产生误报。(144593/CSCze94840)
- 在某些情况下，如果您创建了一条引用已启用**检查本地路由流量 (Inspect Local Router Traffic)** SSL 策略的访问控制策略，系统会出现问题。作为解决方法，请勿启用**检查本地路由流量 (Inspect Local Router Traffic)** 选项。(CSCut12631)
- 在某些情况下，如果您修改无人值守管理 (LOM) 的管理员密码以包含美元字符 (**$**)，系统在不该修改并截断密码的情况下自动更改思科集成管理控制器 (CIMC) 密码并在 **$** 后截断密码。作为解决方法，请在修改 LOM 管理员密码之后使用截断后的密码登录 CIMC，然后将 CIMC 密码修改为正确的长度。(CSCut27442)
- 在 **system file secure-copy** CLI 命令中，支持星号.**(*)** 字符。(CSCuu25329)
- 如果您生成报告，然后离开“报告模板”(Report Templates) 选项卡，“报告”(Reporting) 页面（**概述 [Overview] > 报告 [Reporting]**）中“报告模板”(Report Templates) 选项卡上的“发送邮件”(send email) 复选框不会保持选中状态。(CSCuu41580, CSCuv43116)
- 在某些情况下，如果创建引用网络分析策略的访问控制策略并禁用 Modbus 预处理器，然后启用在“规则编辑器”(Rule Editor) 页面（**策略 [Policies] > 入侵 [Intrusion] > 规则编辑器 [Rule Editor]**）中列出的 Modbus 预处理器的所有 Modbus 规则，系统不会按预期自动启用 Modbus 预处理器。(CSCuu66121)
- 在某些情况下，如果将受管设备的基准设置为带最新漏洞数据库 (VDB) 的版本 5.4.x，并应用网络发现策略，然后通过 Internet Explorer 版本 11 进行浏览，任何事件及“连接事件”(Connection Events) 页面（**分析 [Analysis] > 连接 [Connections] > 事件 [Events]**）的“主机配置文件”(Host Profile) 弹出窗口会错误地使用 Internet Explorer 7 报告事件。(CSCuu67292)

- 在某些情况下，系统会截断包含 36 个或更多字符且分配到访问控制策略的用户名或组名，即使文档声明支持 36 个或更多字符。(CSCuu70235)
- 在某些情况下，当创建 LDAP 对象、下载组和用户时，以及在访问控制策略中，系统可能不会始终支持 UTF8 字符。解决方法是，使用 ACSII 字符在 Microsoft Active Directory 服务器或 LDAP 服务器上创建 LDAP 对象。(CSCuv27375)
- 在 ASA FirePOWER 模块 上不支持 **show user** CLI 命令。解决方法是，使用专家外壳在 **/etc/shadow** 文件中查找用户名。(CSCuv45343)
- 在某些情况下，如果在 DC4000 上注册和管理多个设备，系统可能会遇到连接问题。(CSCuw11462)
- 在某些情况下，系统更新期间防御中心上的登录会话在更新过程完成之前过期，以致于您的系统未能成功更新。解决方法是，点击 Web 界面中的不同选项卡，或创建计划任务，以每小时为间隔下载更新，从而避免会话超时。（CSCuw26878、CSCux04478）
- 在某些情况下，如果在高可用性环境中向主要/活动防御中心注册设备，并在防御中心完成设备同步之前将设备重命名为一个包含超过 39 个字符的名称，向辅助/非活动防御中心注册设备时会失败。(CSCuw27368)
- 在某些情况下，如果创建一个默认操作设置为**交互拦截 (Interactive Block)** 或**交互拦截并重置 (Interactive Block with reset)** 的访问控制规则，点击拦截页面上的**继续 (Continue)** 可能会意外地从 HTTP 网页重定向到 HTTPS 网页。解决方法是，清除网络浏览器上的浏览器缓存，然后点击**继续 (Continue)**。请注意，您可能需要重复该解决方法多次。(CSCuw28868)
- 在某些情况下，如果创建 SSL 策略并从 Windows 操作系统浏览网页，防火墙可能会错误地拦截会话（即使默认操作未设置为**拦截 [Block]**），且系统会遇到问题。(CSCuw36519)
- 在某些情况下，已启用流量配置文件的系统可能遇到磁盘空间问题。(CSCuw74528)
- 在某些情况下，如果创建一个设有**交互拦截 (Interactive Block)** 操作的访问控制规则，系统仅拦截以 **.com** 结尾的网站。(CSCuw92220)
- 如果防御中心耗尽磁盘空间但自行解决了该问题，系统可能仍无法存储和显示新的事件信息，并在“系统日志”(Syslog) 页面（**系统 [System] > 监控 [Monitoring] > 系统日志 [Syslog]**）中生成**分区的所有共享连接均处于繁忙状态 (All shard connections are busy for partition)** 错误。解决方法是重新启动系统。如果系统继续遇到问题，请联系支持部门。(CSCux00142)
- 有时，但是，如果您添加安全区域添加至访问控制策略和应用，系统不正确处理流量。如果您将安全区添加至已应用的访问控制策略，并怀疑您的流量被错误处理或阻止，请禁用访问控制策略中的安全区。(CSCux05653)
- 通过运行版本 5.4.0.5 或更低版本的受管设备将系统更新至版本 6.0，可能会导致流量中断和系统问题。在更新至版本 6.0 之前，必须先将受管设备更新至版本 5.4.0.6 或更高版本。(CSCuy14563)

早期版本中报告了以下已知问题：

- 在某些情况下，如果 Microsoft Windows 更新发生在传输文件的客户端上，该文件检测会失败，因为客户端在单独会话中传输文件片段，而系统无法重组它们以检测完整文件。(112284/CSCze88424)
- 由于数据库检查，系统需要额外时间来重新启动运行 5.3 版本或更高版本的设备或 ASA FirePOWER 模块。如果在数据库检查过程中发现错误，重新启动需要额外时间来修复数据库。（135564、136439）
- 如果在使用 Internet Explorer 11 查看 Web 界面时创建新报告（**概述 [Overview] > 报告 [Reporting] > 报告模板 [Report Templates]**）并尝试插入报告参数，将不会向报告说明部分中添加任何报告参数。解决方法是使用 Internet Explorer 10。(142950/CSCze94011)
- 在某些情况下，如果在通过 ASA 会话命令登录时尝试使用 SFR **system restart** CLI 命令，设备可能会停止进程，且不会重新开始它们。这将影响除 ASA5506-X 以外的所有设备。(143135/CSCze94403)
- 在某些情况下，如果创建一个设有交互拦截操作的访问控制规则，并启用连接开始日志记录或同时启用连接开始和连接结束日志记录，系统会因为**用户绕过 (User Bypass)**.原因而不记录连接开始事件。（143357/CSCze93672、144167/CSCze94675）

- 在某些情况下，如果集群的系列 3设备进入维护模式，然后遇到电源故障，而您尝试重新启动设备，系统将无法恢复。如果您的设备没有从维护模式中成功恢复，请联系支持部门。(143504/CSCze94928)
- 在某些情况下，如果创建一个访问控制规则，其设置为允许引用设为**解密重签 (Decrypt-Resign)** 的 SSL 规则和设为“内联模式下丢弃”(drop when inline) 的入侵规则的流量，系统会在入侵事件表视图（**分析 [Analysis] > 入侵 [Intrusion] > 事件 [Events]**）中将 SSL 状态错误地显示为“未知”(Unknown)。(143665/CSCze94947)
- 在某些情况下，您的访问控制策略可能错误地显示为过期。(14412/CSCze95029)
- 在某些情况下，如果将某个引用两个入侵策略的访问控制策略应用于两台设备，然后编辑第一个入侵策略，将该策略重新应用于一台设备并将两台设备集群在一起，经过修改的入侵策略会在第二台设备上标记为过期。解决方法是，将具有相同入侵策略的不同访问控制策略应用于第二台设备。(144136/CSCze95126)
- 在某些情况下，如果创建一个访问控制策略，其通过 HTTP 响应页面引用设置了“交互拦截”(Interactive Block) 操作的规则，且您尝试访问生成 HTTP 响应页面的 URL，则无法在同一浏览器的其他选项卡中访问同一网页。(144419/CSCze95694)
- 在某些情况下，系统可能不会显示“连接事件”(Connection Events) 表视图（**分析 [Analysis] > 连接 [Connections] > 事件 [Events]**）中以下列的策略相关信息：**操作 (Action)**、**原因 (Reason)**、**访问控制策略 (Access Control Policy)**、**访问控制规则 (Access Control Rule)** 和**网络分析策略 (Network Analysis Policy)**。(145142/CSCze95299)
- 在某些情况下，系统不会在“发现统计信息”(Discovery Statistics) 页面（**概述 [Overview] > 摘要 [Summary] > 发现统计信息 [Discovery Statistics]**）的统计信息摘要的**事件总数 (Total Events)**、**最后一小时的事件总数 (Total Events Last Hour)** 或**最后一天的事件总数 (Total Events Last Day)** 行中显示任何事件。(145153/CSCze95751)
- 在某些情况下，如果生成入侵事件性能图表（**概述 [Overview] > 摘要 [Summary] > 入侵事件性能 [Intrusion Event Performance]**）并选择**最后一小时 (Last Hour)** 作为时间范围，所生成的图表为空，而不是包含入侵事件表视图中的数据。(145237/CSCze95774)
- 打开电源时，您的设备可能会等待较长时间。(145248/CSCze96068)
- 在某些情况下，如果在高可用性配置中的 ASA 5515 模块上启用设置为“仅监控”的故障时打开 Cisco 冗余协议 (SFRP)，且设备遇到故障转移，您的模块可能会多次意外地从主用模式变为备用模式。(145256/CSCze95812)
- 如果使用网络地址转换 (NAT) 配置运行版本 5.0 或更高版本的 ASA FirePOWER 模块，系统会错误地处理与应用的访问控制、入侵和网络发现策略匹配的数据通道。(145274/CSCze96017)
- 在某些情况下，如果在配置了高可用性的系统上“警报”(Alerts) 页面（**策略 [Policies] > 操作 [Actions] > 警报 [Alerts]**）的“高级恶意软件防护警报”(Advanced Malware Protections Alerts) 选项卡中进行更改，可能不会在设备之间正确同步这些更改。(CSCur46711)
- 如果在删除流量配置文件之前未将其停用，系统将允许删除的配置文件持续使用资源，而不生成流量。(CSCur48345)
- 在某些情况下，如果使用思科冗余协议 (SFRP) 配置路由的系列 3受管设备的集群并应用网络地址转换 (NAT) 规则，集群的主要设备和辅助设备会同时响应在匹配流量中检测到的地址解析协议 (ARP)，而正常情况下仅应该由主要设备作出响应。解决方法是，在为集群设备创建 NAT 规则时，指定主要设备上的 SFRP 接口作为主接口，而指定辅助设备上的 SFRP 作为备用接口。(CSCur55568)
- 如果创建计划任务以在防御中心上安装新版本的漏洞数据库 (VDB)，系统将不会在您已安装了最新 VDB 版本的情况下发出警告，且每当计划任务时，防御中心都会从主用模式切换到备用模式。Cisco不建议计划自动 VDB 更新。(CSCur59252)
- 如果在 81xx 子系列设备上的入侵策略中配置 DNS 预处理器时使用无效的 IP 地址，系统功能可能会呈指数降低。要解决此问题，请输入有效的 IP 地址并重新应用入侵策略。(CSCur59598)
- 在某些情况下，如果在虚拟设备上配置一对内联接口，CLI **how traffic-statistics** 命令不会显示内联对中第二个接口的数据。(CSCur59771)

- 在某些情况下，对于可能已过期或已从注册设备中删除的许可证，“设备管理”(Device Management) 页面（**设备 [Devices] > 设备管理 [Device Management]**）的“设备”(Device) 选项卡显示**是 (yes)**，而它应该显示**否 (no)**。(CSCur61884)
- 在某些情况下，如果从许可证页面（**系统 [System] > 许可证 [Licenses]**）删除保护许可证，系统不会按预期递减所用许可证的数量。解决方法是，从“设备管理”(Device Management) 页面（**设备 [Devices] > 设备管理 [Device Management]**）禁用该许可证。(CSCur61927)
- 无法应用在当前应用的访问控制策略中未引用的现有入侵策略。(CSCur72904)
- 在 ASA5506X 设备上检测到的入侵可能不会针对 gzip 压缩的 HTTP 流量或分块的 HTTP 响应数据（而将针对解压数据或非分块数据）生成警报。(CSCur77397)
- 如果以用户身份而非管理员身份登录到系统，并对所应用入侵策略的基层进行编辑，系统会将该策略标记为**管理员**（实际并非管理员）所做的更新。(CSCur79437)
- 在某些情况下，如果系统在应用策略期间丢失了防御中心与设备之间的连接，“网络发现”(Network Discovery) 页面（**策略 [Policies] > 网络发现 [Network Discovery]**）将显示**应用于设备 (apply to devices)**。解决方法是，编辑网络发现策略并重新应用。(CSCur81583)
- 如果创建一个入侵策略，其引用设置为**忽略音频/视频数据通道 (Ignore Audio/Video Data Channel)** 的网络分析策略，系统将针对会话发起协议 (SIP) 音频数据生成警报，而它不应该这样做。(CSCur83184)
- 如果手动将防御中心或受管设备的时间配置为过去的时间，“运行状况监控器”(Health Monitor) 页面（**运行状况 [Health] > 运行状况监控器 [Health Monitor]**）未显示警报。(CSCur85894)
- 在某些情况下，如果将集群的系列 3 受管设备的路由器接口同时配置为私有 IP 地址和 Cisco冗余协议 (SFRP) IP 地址，系统无法识别哪个 IP 地址是主要地址，且不会建立开放最短路径优先 (OSPF) 连接。(CSCur86355)
- 在某些情况下，如果创建一个启用了 HTTP 预处理器和**无限解压 (Unlimited Decompression)** 的网络分析策略，及一个设置为针对 gzip 压缩 HTTP 流量中的数据发出警报的入侵规则，系统可能不会根据所应用的入侵规则针对超过 65535 字节解压数据的流量生成警报。(CSCur87659)
- 在某些情况下，如果在“用户首选项”(User Preferences) 页面上的“时区首选项”(Time Zone Preference) 选项卡（**管理 [Admin] > 用户首选项 [User Preferences] > 时区首选项 [Time Zone Preference]**）中更改选定时区，系统可能不会包括夏令时，且可能会显示错误的时间。(CSCur92028)
- 在某些情况下，如果部署一个大型数据库并尝试在防御中心上创建故障排除文件，系统会对此任务使用额外内存，并生成 **内存不足! (Out of memory!)** 错误。(CSCur97450)
- 如果在更新至版本 5.4.1.1 或更高版本之前未在 DC2000 和 DC4000 设备上运行 BIOS 版本 2.0.1b，更新将失败。如果由于您的防御中心运行的 BIOS 版本过低而导致更新失败，请联系支持部门。(CSCus10407)
- 在检测 Sametime 应用时，您可能会遇到误报。(CSCus17165)
- 无法在 ASA5585X 设备上重置管理员用户的密码。(CSCus17991)
- 系统日志消息中未填充以下字段的信息：HTTP Referrer、用户代理 (User Agent) 和引用的主机 (Referenced Host)。(CSCus18179)
- 在系统上运行故障排除可能会导致延迟。(CSCus19876)
- 在某些情况下，如果与事件关联的主机已停用，将无法从危害表现 (IOC) 表视图（**分析 [Analysis] > 主机 [Hosts] > 危害表现 [Indications of Compromise]**）中删除或解析 IOC。(CSCus24116)
- 在某些情况下，如果在所应用的 SSL 策略中引用了一个受信任的证书授权 (CA) 组或对象，系统不允许您从策略中删除该组或对象。解决方法是，向策略中添加一个不同的 CA 组或对象，然后从当前 SSL 策略中删除受信任的 CA 组或对象。(CSCus42239)
- 如果运行版本 5.4.1 的 ASA5506-X 设备未安装 URL 许可证，或者如果许可证不可用，“云服务”(Cloud Services) 页面（**系统 [System] > 本地 [Local] > 配置 [Configuration]**）会错误地显示带有时间戳的**上次 URL 过滤更新 (Last URL filtering update)** 消息。(CSCus51935)

- 在某些情况下，如果创建一个单独的 URL 对象并将该单独对象添加到 URL 组对象中，然后修改组对象，该单独对象的工具提示未反映组对象的更新值。(CSCus51943)
- 在某些情况下，如果您的 URL 许可证不可用或已删除，而您尝试添加新的 URL 许可证，“云服务”(Cloud Services) 页面（**系统 [System] > 本地 [Local] > 配置 [Configuration]**）上的**启用自动更新 (Enable Automatic Updates)** 选项不会按预期默认为选中状态。(CSCus53842)
- 在某些情况下，如果安装新的入侵规则更新，然后将备份还原到设备，系统会错误地生成**入侵策略已过期 (Intrusion Policy is out-of-date)** 消息，而不管入侵策略存在于规则更新之前还是之后。(CSCus59479)
- 在某些情况下，如果您的访问控制策略所含的源地址和目标地址中包括 **::/0**，则连接事件表视图（**分析 [Analysis] > 连接 [Connections] > 事件 [Events]**）包含从 IPv4 和 IPv6 流量生成的事件，而正常情况下仅应允许 IPv6 流量。(CSCus63549)
- 如果无法通过授权代理连接到思科云，但可以进行直接连接，请联系支持部门。(CSCus83379)
- 在某些情况下，如果将某个访问控制策略应用于防御中心中的 ASA5506X 设备，且该策略与多个启用了许多规则的入侵策略关联，策略应用将失败。解决方法是使用较少策略。入侵策略和变量集的每个唯一组合均视为一个策略，与访问控制策略关联的网络访问策略也视为一个策略。(CSCus95519)
- 解决了以下问题：如果在启用了动态分析的情况下创建一个包含文件策略的访问控制策略，且代理端口配置为端口 80，则动态分析所需的综合安全智能云失败。(CSCut01361)
- “备份/还原”(Backup/Restore) 页面（**系统 [System] > 工具 [Tools] > 备份/还原 [Backup/Restore]**）的“备份管理”(Backup Management) 选项卡不包括注册的 ASA55X5 或 ASA55X5-SSP-XX 设备作为选项。(CSCut41338)
- 在某些情况下，如果将某个思科 IOS 空路由实例添加到思科 IOS 补救措施中，并启用密码以登录到路由器，设备将不会启用密码，且补救措施将失败。解决方法是，不要选择启用密码。(CSCus45769)
- 如果应用一个引用安全智能 (SI) 对象的访问控制策略，且策略应用失败，请重新应用访问控制策略。如果您仍然无法应用策略，请联系支持部门。(CSCus50470)
- 在某些情况下，如果为 Nmap 模块设置一个扫描实例，远程操作系统检测可能会错误地识别检测到的操作系统的版本。解决方法是，参阅主机脚本输出以获取正确的操作系统。(CSCut23654)
- 在某些情况下，如果应用一个引用之前已删除的网络对象或组的访问控制规则，高可用性配置中的防御中心将无法识别该网络对象或组已删除且遇到问题。解决方法是，删除包含已删除对象或组的规则并使用对象重新创建规则，然后应用策略。(CSCut54187)
- 系统不支持集群的系列 3设备上配置的虚拟路由器接口具有多个常规 IP 地址。(CSCut58601)
- 在某些情况下，如果在高可用性配置中更新一对防御中心，辅助防御中心的访问控制策略可能显示为最新，而主要防御中心的访问控制策略不显示为最新。请注意，系统应报告访问控制策略所引用的对象和策略的正确状态。(CSCut63260)
- 在某些情况下，如果针对生成的事件创建并编辑搜索，然后在搜索开始之前取消搜索，系统会将您重定向到与搜索相关的事件页面，并显示错误的搜索名称。(CSCut63265/CSCuu97738)
- 在某些情况下，如果 rna 映射列表中的最后一个条目重复，则网络映射会遇到问题。如果您遇到 SFDatacorrelator 性能问题，请联系支持部门。(CSCut65738)
- 在某些情况下，云查找会生成无关警报。(CSCut77594)
- 在某些情况下，如果系统连续两次出现故障，系统可能会进入旁路模式，即使这是为非旁路模式专门配置的。(CSCut80892)
- 如果您尝试在 Chrome 浏览器上选择“应用过滤器”(Application Filters) 页面（**对象 [Object] > 对象管理 [Object Management] > 应用过滤器 [Application Filters]**）中的所有应用过滤器（通过选择第一个可用的应用过滤器，然后使用键盘命令按住 Shift 键并点击最后一个可用的应用过滤器），将仅选中所选的两个应用过滤器。您必须单独选择每个应用，才能包括所有可用的过滤器。(CSCut86012)

- 如果将以下具备 FirePOWER 服务的 Cisco ASA 从版本 5.4.1 更新至版本 5.4.1.1，FirePOWER 服务在更新过程中不可用：ASA5506-X、ASA506H-X、ASA5506W-X、ASA5508-X、ASA5516-X。FirePOWER 服务在设备更新完成后可用。解决方法是，通过 SSH 使用 **tail -f /var/log/sf/Cisco_network_sensor_Patch-5.4.1.1_main_upgrade_script.log** 命令观察更新过程，并在更新完成后重新启动 ASA 模块上的自适应安全设备管理器 (ASDM)。(CSCut89599)
- 在某些情况下，如果在系统重新启动时为内联部署配置的感应接口关闭，Snort 会持续重新启动。(CSCut93464)
- 在某些情况下，如果启用在连接了注册设备的系统上配置的多个接口，并在设备上使用 **show managers** CLI 命令，系统将显示错误的 IP 地址。(CSCut95947)
- 在某些情况下，您的 3D8xx 设备可能会遇到错误，并失去控制和信息通道。(CSCut98395)
- 如果在选择了**删除 <设备名称> 上的接口配置 (Remove the interface configurations on <device name>)** 选项的情况下拆分一个包含 NAT 策略的设备集群，拆分该集群后，将无法在辅助设备上应用策略。解决方法是，在分离集群设备时，取消选择**删除 <设备名称> 上的接口配置 (Remove the interface configurations on <device name>)**。(CSCut98774)
- 如果您尝试更新设备，但在更新后遇到系统问题（如无法访问设备），请联系支持部门。(CSCuu01055)
- 如果您使用 **system support run-rule-profiling** CLI 命令，且发生堆栈跟踪，请重新应用访问控制策略。(CSCuu02211)
- 在某些情况下，如果禁用某个引用入侵策略的访问控制规则，在成功重新应用该访问控制策略后，“访问控制” (Access Control) 页面（**策略 [Policies]** > **访问控制 [Access Control]**）会错误地将入侵策略显示为过期。“入侵策略” (Intrusion Policy) 页面（**策略 [Policies]** > **入侵 [Intrusion]** > **入侵策略 [Intrusion Policy]**）将显示正确的策略状态。(CSCuu15483)
- “文件轨迹” (File Trajectory) 页面（**分析 [Analysis]** > **文件 [Files]** > **网络文件轨迹 [Network File Trajectory]**）将具有危害表现的主机的第一个和最后一个主机图标显示为蓝色图标，而不是红色图标。(CSCuu17950)
- 在某些情况下，如果向防御中心注册 ASA FirePOWER 模块并重新启动 ASA FirePOWER 模块，防御中心与虚拟 ASA 设备上的 VMware 工具之间的数据通道连接将发生中断。解决方法是，重新注册您的 ASA 设备。(CSCuu18450)
- 在某些情况下，如果创建一个文件策略和一个 NAT 策略并启用 TCP 数据流预处理器规则，而其 HTTP 端口号不是网络访问策略的 HTTP 预处理器配置页面中的可用端口，系统将不会检测到与文件策略配置操作匹配的流量中的恶意软件，并下载恶意软件内容（而它不应该这样）。(CSCuu24472)
- 在某些情况下，如果您启用了至少两个管理接口且系统丢失了与其中一个接口的连接，系统将默认为错误的网关 IP 地址，且您无法访问该接口。(CSCuu44020)
- 在某些情况下，如果创建一个包含地理位置条件的访问控制策略，应与该条件匹配的流量将无法匹配。(CSCuu48800)
- 在某些情况下，如果在向防御中心注册设备后更新设备，使用 **configure manager <IP address> add** CLI 命令会禁止防御中心管理该设备。解决方法是，在更新后等待设备自动向防御中心进行注册。(CSCuu44265)
- 在某些情况下，如果在设备上使用 **system file copy** CLI 命令，您可能无法退出 CLI 提示符。解决方法是，使用 **ctr+c** 将命令退回至提示符。(CSCuu48793)
- 在某些情况下，如果您的系统长时间累积大量流量，可能会发生延迟和流量中断。(CSCuu52545)
- 在某些情况下，如果在“入侵事件” (Intrusion Events) 页面（**分析 [Analysis] > 入侵 [Intrusion] > 事件 [Events]**）使用一个无效的子网 IP 地址按**原始客户端 IP (Original Client IP)** 进行过滤，系统会错误地排除没有原始客户端 IP 的入侵事件。(CSCuu68438)
- 如果使用 MAC 地址配置主机输入，系统不会正确存储 MAC 地址，且不会在“发现事件” (Discovery Events) 页面（**分析 [Analysis] > 主机 [Hosts] > 发现事件 [Discovery Events]**）中生成“MAC 地址” (MAC Address) 字段。(CSCuu90757)
- 如果您向防御中心注册了多个设备，尝试连接到 MySQL 时可能会失败。(CSCuu94784)

- 在某些情况下，当您的网络浏览器用于高容量媒体（如视频流）时，系统不会在“摘要控制面板”(Summary Dashboard)（**概述 [Overview] > 控制面板 [Dashboard] > 摘要控制面板 [Summary Dashboard]**）上的“看到的热门 Web 应用”(Top Web Applications Seen) 和“看到的热门客户端应用”(Top Client Applications Seen) 构件中显示正确的字节数。(CSCuu97036)
- 在某些情况下，如果创建一个设有交互拦截操作的访问控制规则，查看拦截的网页并选择**继续 (Continue)** 按钮以绕过拦截，系统可能会将页面从 http:// address 重定向到 https:// address，且网页无法重新加载。(CSCuu97946)
- 如果使用包含空格的文件名创建备份，将该备份应用于防御中心会失败。解决方法是，不要在备份文件名中包含空格。(CSCuu99818)
- 如果某个用户属于 LDAP 用户感知对象中包含的组，但用户所属的组在 Active Directory 服务器上设置为主要组，则该用户不包含在从 Active Directory 服务器下载的访问控制用户列表中，且您无法将该用户添加到访问控制规则中。(CSCuv03821)
- 在某些情况下，如果在“报告模板”(Report Templates) 页面（**概述 [Overview] > 报告 [Reporting] > 报告模板 [Report Templates]**）中生成具有修改的**最大结果 (Maximum Results)** 值的连接事件报告，系统会生成具有默认值（而非修改值）的报告。(CSCuv06557)
- 在某些情况下，如果创建一个虚拟路由器过滤器，系统会错误地将虚拟路由器 OSPF 路由类型另存为 **Ext-2** 而非 **Ext-1**。(CSCuv08158)
- 在某些情况下，如果配置一个系统策略，以便使用远程 NTP 服务器将时间同步到连接了注册的 ASA 5500-X 设备、系列 2设备或系列 3 设备（运行低于 5.4 的版本）的系统，且遇到跳秒，系统可能会使用大量 CPU。(CSCuv11738)
- 在某些情况下，如果创建一个具有交互拦截操作的访问控制规则，并在 Chrome 网络浏览器中查看拦截的网页，选择**继续 (Continue)** 按钮以绕过拦截页面将不起作用。解决方法是，使用 Firefox 或 Internet Explorer 查看拦截的网页。(CSCuv21748)
- 在某些情况下，如果添加一个集群并编辑接口，您将无法编辑辅助接口，且系统会生成**无法加载容器 (Unable to load container)** 错误。(CSCuv25142)
- 如果在“对象管理”(Object Management) 页面（**对象 [Objects] > 对象管理 [Object Management] > PKI**）中生成新的内部 CA 证书，生成的证书有效期仅为 30 天，而有效期应该为十年。(CSCuv29004)
- 在某些情况下，如果编辑网络发现策略的危害表现 (IOC) 设置，然后禁用 IOC 并保存更改，IOC 仍会显示在“按主机列出的危害表现”控制面板构件中。(CSCuv41376)
- 在某些情况下，如果创建一个配置了选作目标或源国家/地区的所有国家/地区的访问控制规则，系统不会匹配 IPv6 流量。解决方法是，创建一个配置了选作目标或源国家/地区的单个国家/地区的访问控制规则。(CSCuv93913)
- 在某些情况下，如果在设备上配置一个静态路由，并重新应用您的系统策略，系统会错误地删除该静态路由。(CSCuw07826)
- 如果在“捕获的文件摘要”(Captured File Summary) 工作流程（**分析 [Analysis] > 文件 [Files] > 捕获的文件 [Captured Files]**）的表视图中点击一个包含扩展字符的文件名，将会发生内部服务器错误。(CSCuv40941)
- 在某些情况下，SFDatacorrelator 会发生问题，且不会正确处理 Snort 消息。(CSCuw34423)
- 在某些情况下，如果尝试从“安全区”(Security Zones) 页面（**对象 [Objects] > 对象管理 [Object Management] > 安全区 [Security Zones]**）删除在 ASA5500X 系列设备所应用的访问控制策略中引用的安全区，系统将不会保存更改，且不会删除该安全区。解决方法是，从访问控制策略中移除安全区，然后从“安全区”(Security Zones) 页面删除该安全区。(CSCuv40232)
- 如果在不包含任何发现事件的防御中心上打开“发现统计信息”(Discovery Statistics) 页面（**概述 [Overview] > 摘要 [Summary] > 发现统计信息 [Discovery Statistics]**），将会发生内部服务器错误。(CSCuv42327)

获取帮助

感谢您选用 FireSIGHT 系统。

Cisco支持

有关获取文档、使用 Cisco 漏洞搜索工具 (BST)、提交服务请求和收集 Cisco ASA 设备其他相关信息的内容，请参阅*《思科产品新特性文档》*，网址为：http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html。

请订阅*《思科产品新特性文档》*，该内容以 RSS 源的形式列出所有新的和经过修订的 Cisco 技术文档，并通过阅读器应用直接将内容提供至您的桌面。RSS 源是一种免费服务。

如果有任何疑问或者需要 Cisco ASA 设备方面的帮助，请通过以下方式联系 Cisco 支持部门：

- 请访问 Cisco 持站点，网址为：http://support.cisco.com/。
- 将问题发送至 Cisco技术支持部门的邮箱：tac@cisco.com。
- 致电 Cisco支持部门，电话号码为：1.408.526.7209 或 1.800.553.2447。

获取文档和提交服务请求

有关获取文档、使用思科缺陷搜索工具 (BST)、提交服务请求和收集其他信息的信息，请参阅*思科产品文档更新*，其网址为：http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html。

订用*思科产品文档更新*，其中将所有最新及修订的思科技术文档列为 RSS 源并通过使用阅读器应用将相关内容直接发送至桌面。RSS 源是一种免费服务。