



# FireSIGHT 系统版本说明

版本 5.4.0.4 和版本 5.4.1.3

首次发行日期：2015 年 9 月 28 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、3D6500、3D1000、3D2000、3D2100、3D2500、3D3500、3D4500、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 以及 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：**您无法将适用于 Blue Coat X 系列的 Cisco NGIPS 上运行的 FireSIGHT 系统版本 5.3.0.x 直接更新为版本 5.4。而必须先卸载旧版本，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*》。从版本 5.4 开始不适用。

**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 FireSIGHT 系统版本 5.4.0.4 和版本 5.4.1.3。物理和虚拟受管设备可更新为版本 5.4.0.4。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 5.4.1.3。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）当前不支持版本 5.4.1.3；必须先运行版本 5.4，才能更新至版本 5.4.1.3。如果防御中心运行的是较低版本，必须先更新为版本 5.4，然后才能更新为版本 5.4.1.3。  
**说明：**运行版本 5.4.1.1 的防御中心可以更新其设备，但如果您的防御中心运行的仍是版本 5.4，您将无法解密或检测 SSL 流量。如果您要解密或检测 SSL 流量，请将您的防御中心更新至版本 5.4.1.3
- 系列 2 设备（3D500、3D1000、3D2000、3D2100、3D2500、3D3500、3D4500 和 3D6500）必须运行版本 5.4 才能更新为版本 5.4.0.4。如果系列 2 设备运行的是较低版本，必须先更新为版本 5.4，然后才能更新为版本 5.4.0.4。
- 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 才能更新为版本 5.4.0.4。如果系列 3 设备运行的是较低版本，必须先更新为版本 5.4，然后才能更新为版本 5.4.0.4。
- 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 5.4.0.4。如果 ASA FirePOWER 模块运行的是较低版本，必须先更新为版本 5.4，然后才能更新为版本 5.4.0.4。ASA FirePOWER 模块（ASA5506-X、ASA5506W-X、ASA5506H-X、

## 新功能

ASA5508-XASA5516-X 和 ISA 3000) 必须先运行版本 5.4.1 或更高版本, 才能更新至版本 5.4.1.3。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, 第 2 页](#)
- [文档更新, 第 8 页](#)
- [准备工作: 重要更新和兼容性说明, 第 8 页](#)
- [安装更新, 第 13 页](#)
- [已解决的问题, 第 18 页](#)
- [已知问题, 第 26 页](#)
- [获取帮助, 第 33 页](#)

## 新功能

版本说明中的该节汇总了 FireSIGHT 系统版本 5.4.0.4 和版本 5.4.1.3 中新增及更新的特性和功能:

- [术语, 第 2 页](#)
- [早期版本中引入的特性和功能, 第 3 页](#)

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

如果您参阅版本 5.3.1.x 或 5.3.0.x 的相应文档, 可能会注意到这些文档中使用的术语与版本 5.4.0.4 和版本 5.4.1.3 中的术语有所不同。

表 1 术语更改

适用于版本 5.4.0.4 和版本 5.4.1.3 的术语	说明
Cisco	原称为 <i>Sourcefire</i>
FireSIGHT 系统	以前是 <i>Sourcefire 3D 系统</i>
防御中心 FireSIGHT 防御中心 Cisco FireSIGHT 管理中心	原称为 <i>Sourcefire 防御中心</i>
设备 受管设备	以前是 <i>Sourcefire 受管设备</i>
适用于 Blue Coat X 系列的 Cisco NGIPS	原称为 <i>用于 X 系列的 Sourcefire 软件</i>
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)
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

表 1 术语更改 (续)

适用于版本 5.4.0.4 和版本 5.4.1.3 的术语	说明
自适应安全设备管理器 (ASDM)	是指用于管理 ASA 功能的自适应安全设备管理器
直接管理	是指使用 ASDM 管理 ASA5506-X 上的 ASA FirePOWER 模块
集中管理	是指使用 FireSIGHT 管理 ASA5506-X 上的 ASA FirePOWER 模块防御中心

**提示：** Cisco 文档可能将防御中心称为 FireSIGHT 管理中心。防御中心和 FireSIGHT 管理中心是同一个设备。

## 早期版本中引入的特性和功能

### 版本 5.4.1.1

#### 专用 AMP 设备

版本 5.4 引入了新的系列 3 FirePOWER 受管设备，旨在增强处理能力，以最大限度的提升 FireSIGHT 系统的 AMP 功能的性能。AMP8050 是 81xx 子系列设备，支持网络模块，具有作为专用 AMP 设备正常运行所需的附加存储。AMP8350 是 83xx 子系列设备，也支持网络模块，具有 AMP 功能所需的附加存储。AMP8350 型号可与 AMP8360、AMP8370 和 AMP8390 组成堆叠设备，这些组合分别适用于 2 个、3 个和 4 个堆栈。

#### FirePOWER 服务管理功能

##### 集中管理具备 FirePOWER 服务的 Cisco ASA

防御中心现在能够以与管理所有其他 ASA5500-X 设备相同的方式管理运行于 ASA5506-X、ASA5506W-X、ASA5506H-X、ASA5508-X 和 ASA5516-X 设备的 FirePOWER 服务 (ASA FirePOWER 设备)。这样只要 ASA 平台运行 9.3.1 版或更高版本，且 ASA FirePOWER 设备运行版本 5.4.1 或更高版本，就可以从单个防御中心管理运行 ASA FirePOWER 设备的多台 ASA 设备。管理员可以配置入侵检测和防御策略、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，然后将这些配置同时应用于多台 ASA 设备。此外，防御中心在单个视图中提供关键控制面板、事件视图、告警功能以及来自所有 ASA FirePOWER 设备的报告。

##### 直接管理具备 FirePOWER 服务的 Cisco ASA

Cisco 自适应安全设备管理器 (ASDM) 可用于执行上述 ASA FirePOWER 管理功能，但一次只能管理一台 ASA 设备 (ASA5506-X、ASA5506W-X、ASA5506H-X、ASA5508-X 和 ASA5516-X)。此外，您可以直接管理系统策略、许可、备份和还原。

##### 具备 FirePOWER 服务的 Cisco ASA 的管理限制

目前，Cisco ASA FirePOWER 产品由两款相互紧密集成的产品组成：ASA 防火墙和 FirePOWER 下一代入侵防御系统 (NGIPS)。虽然这两款产品之间已实现关键数据共享，但统一管理平台仍在开发中。

由于这个原因，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任何功能：

- 基于 Cisco ASA 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 LAN 接口。此外，如果 FirePOWER 服务是在 SPAN 端口模式下部署，配置的任何 ASA 接口都不会显示。
- 关闭、重启或管理 ASA 流程。
- 从 ASA 设备创建或还原备份。
- 使用 VLAN 标记条件编写访问控制规则来匹配流量。

**说明：** ASA 平台提供上述功能，并可通过 ASA 命令行界面 (CLI) 和 ASDM 对其进行配置。有关详细信息，请参阅 ASA FirePOWER 模块文档。

## 版本 5.4.1:

### FirePOWER 服务管理功能

#### 集中管理具备 FirePOWER 服务的 Cisco ASA5506-X

防御中心现在能够以与管理所有其他 ASA5500-X 设备相同的方式管理运行于 ASA5506-X 设备上的 FirePOWER 服务（ASA FirePOWER 设备）。这样只要 ASA 平台运行的是 9.3.1 版或更高版本，且 ASA FirePOWER 设备运行的是版本 5.4.1 或更高版本，就可以从单个防御中心管理运行 ASA FirePOWER 设备的多台 ASA5506-X 设备。管理员可以配置入侵检测和防御策略、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，然后将这些配置同时应用于多台 ASA5506-X 设备。此外，防御中心在单个视图中提供关键控制面板、事件视图、告警功能以及来自所有 ASA FirePOWER 设备的报告。

#### 直接管理具备 FirePOWER 服务的 Cisco ASA5506-X

Cisco 自适应安全设备管理器 (ASDM) 可用于执行上述 ASA FirePOWER 管理功能，但一次只能管理一台 ASA5506-X 设备。此外，您可以直接管理系统策略、许可、备份和还原。

#### 具备 FirePOWER 服务的 Cisco ASA 的管理限制

目前，Cisco ASA FirePOWER 产品由两款相互紧密集成的产品组成：ASA 防火墙和 FirePOWER 下一代入侵防御系统 (NGIPS)。虽然这两款产品之间已实现关键数据共享，但统一管理平台仍在开发中。

由于这个原因，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任何功能：

- 基于 Cisco ASA 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 LAN 接口。此外，如果 FirePOWER 服务是在 SPAN 端口模式下部署，配置的任何 ASA 接口都不会显示。
- 关闭、重启或管理 ASA 流程。
- 从 ASA 设备创建或还原备份。
- 使用 VLAN 标记条件编写访问控制规则来匹配流量。

**说明：**ASA 平台提供上述功能，并可通过 ASA 命令行界面 (CLI) 和 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

现在 VMware 工具可与 FireSIGHT 系统虚拟设备配合使用。这样可实现软关机、迁移及其他特定于虚拟设备的功能，从而增强与 VMware 环境之间的兼容性，并改善虚拟设备管理。以下设备支持 VMware 工具：

- 64 位虚拟防御中心
- 64 位虚拟受管设备

**说明：**从版本 5.4 开始，FireSIGHT 系统支持 ESXi 版本 5.1 和 5.5。

#### VMware 虚拟设备支持 VMXNET3 接口

虚拟设备现在支持 VMXNET3 接口类型，这样您可以使用带宽高达 10Gbps 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。可以将一个接口设置为用于传输管理流量，另一个接口设置为用于传输事件流量。这样可改进某些环境中的部署选项。

#### 系列 3 支持

版本 5.4 引入了 3D7050 作为 70xx 子系列设备，该设备搭载双核四线程处理器，具有 8GB RAM 和 80GB 硬盘。

## 新功能

### 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，以将多条链路汇聚成一条链路。这样可实现链路冗余和带宽共享。

### 防御中心 2000 (DC2000)

DC2000 是新推出的防御中心设备平台，其性能和容量是 DC1500 的两倍。

### 防御中心 4000 (DC4000)

DC4000 是新推出的防御中心设备平台，其性能和容量是 DC3500 的两倍。

## 提升国际兼容性

### Unicode 支持

系统现在会显示通过文件检测、恶意软件检测和 FireAMP 文件事件检测到的文件名。这样可以显示非西文字符（包括双字节编码字符）。

### 关联规则中的地理位置数据和安全情报数据

关联规则引擎经过更新，可提供连接数据、地理位置数据和安全情报数据。这样，您可以根据这两个新的约束生成关联事件或采取关联操作。例如，如果从特定国家/地区检测到 Impact 1 入侵事件，您可以设置警报，将这些信息记录到外部系统日志服务器。

### 支持 FireAMP 私有云

有了版本 5.4，您可以使用 FireAMP 私有云而非思科公共云。要使用 FireAMP 私有云，需要安装私有云虚拟设备。私有云协调与公共云之间的交互，使您可以从公共云收集威胁信息，而且不会泄露您所用网络上的信息。

版本 5.4 更新了以下特性和功能：

## 检测和安全增强功能

### 集成式 SSL 解密

FirePOWER（系列 3）设备现在可以先识别 SSL 通信和解密流量，再应用攻击检测、应用检测和恶意软件检测。您可以在任何受支持的系列 3 设备部署模式下（包括内联和被动模式）使用 SSL 解密。SSL 策略用于控制企业内部使用的 SSL 的特性，其中的 SSL 规则用于对加密流量日志记录和处理实行精细控制。

### 简化了规范化和预处理器配置

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，尤其对于新用户来说。敏感数据预处理程序、规则状态、警报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

新增的 **file\_type** 关键字现可用于 Snort 规则中，该规则允许指定文件类型进行查找。这是现有 **flowbits** 驱动方法的简化替代方法。

### 扩展了来自 FireAMP 连接器的 IoC 支持

FireAMP 提供的危害表现 (IoC) 列表现在是动态且通过数据驱动的。当有新的 IoC 可用时，防御中心会自动支持它们。这在任何采用 FireAMP 的部署中均可增强 IoC 关联功能。

### 受保护的规则内容

Snort 规则语言新增了一项适用于高安全性环境的功能。您现在可以使用哈希数据创建 Snort 内容匹配。这样，规则编写人员可以指定要搜索的内容，但绝不会泄露纯文本内容。

## 先前更改的功能

版本 5.4.1.2 引入了以下功能：

- 您必须将相同的访问控制策略应用于要组成堆栈或集群的所有设备，才能配置堆栈或集群。
- 您现在可以选择在应用策略的过程中不检查流量，以防止网络中断。
- 系统不再将发现事件状态报告至“运行状况策略” (Health Policy) 页面。
- 您现在可以创建引用访问控制规则网络条件集的访问控制策略，以拦截包含 ::/0 的所有 IPv6 地址；或者创建引用网络规则集的访问控制策略，以拦截包含 0.0.0.0/0 的所有 IPv4 地址。
- 现在，当 CPU 使用率从高水平变为正常状态时，系统会为所有 CPU 报告进行事件报告。

版本 5.4.1.1 引入了以下功能：

- 现在，当您上传入侵规则或安装入侵规则更新时，系统会清除所有入侵策略锁定。

版本 5.4.1 引入了以下功能：

- 现在“设备管理” (Device Management) 页面 (**设备 (Devices) > 设备管理 (Device Management)**) 的“高级” (Advanced) 选项卡中提供已注册 ASA 设备的可配置高级选项。
- ASA 设备现在支持 **show users** CLI 命令。
- 在“告警”页面的“高级恶意软件防护告警” (Advanced Malware Protections Alerts) 选项卡中，只能针对追溯性事件或基于网络的恶意软件事件配置告警。

版本 5.4 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。
- 系统现在会识别通过 FTP、HTTP 和 MDNS 协议进行的登录尝试。
- 您限制可以单独从发现事件选择存档的连接事件，并将所选的事件传输到 eStreamer 客户端。
- 运行状况策略中不再提供发现事件运行状况监控器。
- 先前在版本 4.10.x 中提供的“扩展数据包视图” (Expand Packet View) 现可在版本 5.4 的“事件查看设置” (Event View Setting) 选项卡 (**管理 (Admin) > 用户首选项 (User Preferences) > 事件视图设置 (Event View Settings)**) 中进行配置。
- 现在以 **.rtf** 文件导入自定义入侵规则会生成**无效规则文件“rtf\_rule.rtf”**：必须是 ASCII 或 UTF-8 编码的纯文本文件警告。
- 现在您可以通过“入侵事件图表” (Intrusion Event Graphs) 页面 (**概览 (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

## 新功能

- 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
  - TCP 数据包阻止条件规范化
  - 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 紧急标记规范化
- 现在，当配置显示列时，您可以在“连接事件” (Connection Events) 和“安全情报事件” (Security Intelligence Events) 表视图中配置 **HTTP 引用 (HTTP Referrer)** 和 **用户代理 (User Agent)** 字段。
  - 现在您可以通过“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中各个规则相关的警告。在访问控制策略编辑器中，将鼠标指针悬停在规则名称旁边的警报图标上，并读取工具提示文本中的警告，或者选择页面顶部的 **显示警告 (Show Warnings)** 按钮，便可查看与您的访问控制策略中引用的所有规则相关的警告。
  - 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，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 更新为版本 5.4 不会更改内联规范化设置。
  - 您现在可以添加访问控制规则端口条件，用以指定不包含在 **协议 (Protocol)** 下拉列表中的未分配的协议号。
  - 您不再需要在访问控制策略中使用辅助规则来控制 FTP 数据信道。
  - 新增的 **解压缩 SWF 文件 (LZMA)**、**解压缩 SWF 文件 (缩小)** 和 **解压缩 PDF 文件 (默认)** HTTP 预处理器检查选项，为 PDF 和 SWF 文件内容提供更完善的解压缩支持。
  - TCP 流预处理器现在对于 SMTP、POP3 和 IMAP 协议具有更好的感知能力。
  - 系统现在对于应用流量中的信息具有更强的检测能力，包括检测 DNS 流量中的应用数据，以及检测使用其他协议的用户。
  - 您现在可以将 LDAP 身份验证配置为使用通用访问卡 (CAC)，并将所用的 CAC 与用户名关联，这样，用户使用该访问卡便可直接登录系统。
  - 系统增强了 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 5.4.0.4 和版本 5.4.1.3 中，以下文档进行了更新，以反映功能的新增和更改情况，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》

在版本 5.4.0.4 和版本 5.4.1.3 中更新的文档包含以下错误：

- 《FireSIGHT 系统用户指南》包含如下错误表述：**您可以通过 LAN 上串行 (SOL) 连接在默认 (eth0) 管理接口上使用无人值守管理 (LOM) 来远程监控或管理系列 3 设备。**目前不支持使用同一 IP 来进行 LOM 以及通过 SOL 连接系列 3 设备。
- 《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多个变量集配对。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次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”以及在部署安装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 系统虚拟安装向导》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 5.4.0.4 和版本 5.4.1.3 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段或者当中断对部署的影响最小时进行更新。

有关详细信息，请参阅以下各节：

- [配置和事件备份准则，第 8 页](#)
- [更新期间的流量和检查，第 9 页](#)
- [更新过程中的审计日志记录，第 9 页](#)
- [更新至版本 5.4.0.4 和版本 5.4.1.3 的版本要求，第 10 页](#)
- [更新至版本 5.4.0.4 和版本 5.4.1.3 的时间和磁盘空间要求，第 10 页](#)
- [更新至版本 5.4.0.4 和版本 5.4.1.3 后的产品兼容性，第 11 页](#)
- [还原为上一版本，第 12 页](#)

## 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：**防御中心会清除在先前更新中所做的本地存储备份。要保留存档的备份，请将备份存储到外部。

**注意：**DC2000 和 DC4000 设备必须运行 BIOS 版本 2.0.1b，才能更新至版本 5.4.0.4。如果由于 BIOS 版本不兼容而导致设备更新失败，请联系支持部门。

## 更新期间的流量和检查

更新过程将使受管设备重新启动。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 <b>可配置旁路</b> 选项)	<p>网络流量会在更新过程中的两个时间点发生中断：</p> <ul style="list-style-type: none"> <li>■ 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。</li> <li>■ 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。</li> </ul> <p>虚拟设备、适用于 Blue Coat X 系列的 Cisco NGIPS、具备 FirePOWER 服务的 Cisco ASA、8000 系列设备上的非旁路网络模块或 71xx 子系列设备上的 SFP 收发器不支持可配置旁路选项。</p>
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计日志中。

## 更新至版本 5.4.0.4 和版本 5.4.1.3 的版本要求

要更新至版本 5.4.1.3，防御中心必须运行版本 5.4 不支持版本 5.4.1.3。运行版本 5.4.1.1 的防御中心可管理运行版本 5.4.0.4 和版本 5.4.1.3 的设备。如果运行的是较低版本，可从支持站点获取更新。

防御中心必须运行版本 5.4 或更高版本，才能将其管理的设备更新至版本 5.4.1.3。

设备或 ASA 模块的当前版本与发行版本（版本 5.4.0.4 或版本 5.4.1.3）越接近，更新所需的时间就越少。

**注意：**DC2000 和 DC4000 必须运行 BIOS 版本 2.0.1b，才能将设备更新至版本 5.4.0.4 或版本 5.4.1.3。如果由于 DC2000 或 DC4000 运行较低版本的 BIOS 而导致设备更新失败，请联系支持部门。

## 更新至版本 5.4.0.4 和版本 5.4.1.3 的时间和磁盘空间要求

下表提供了版本 5.4.0.4 和版本 5.4.1.3 更新的磁盘空间和时间准则。请注意，使用防御中心更新受管设备时，防御中心的 /Volume 分区需具有额外的磁盘空间。

**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 2 受管设备	126 MB	5946 MB	1141 MB	111 分钟
系列 3 受管设备	225 MB	8337 MB	1520 MB	65 分钟
系列 3 防御中心	300 MB	5327 MB	n/a	154 分钟
适用于 Blue Coat X 系列的 Cisco NGIPS	3655 MB	/mnt/aplocaldisk 上 53 MB	997 MB	37 分钟
虚拟防御中心	300 MB	5327 MB	n/a	因硬件而异
虚拟受管设备	304 MB	3935 MB	1007 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	97 MB	3504 MB	1007 MB	46 分钟
ASA5506-X、ASA5506W-X、 ASA5506H-X、ASA5508-X、 ASA5516-X 和 ISA 3000 上的具备 FirePOWER 服务的 Cisco ASA	9 MB	3500 MB	695 MB	116 分钟

## 更新至版本 5.4.0.4 和版本 5.4.1.3 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 5.4.1.3 的设备。要管理 ASA5506-X、ASA5506W-X、ASA5506H-X、ASA5508-X、ASA5516-X 或 ISA 3000 上的 ASA FirePOWER 模块设备，您**必须**使用运行 5.4.1 版或更高版本的防御中心。

**表 4 管理版本要求**

设备	要由运行版本 5.4.1.3 的防御中心管理时需满足的最低版本
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 系统的版本 5.3
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 和 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 直接更新至版本 5.4。而必须先卸载旧版本，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 5.4.1.3 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 9.3.1 版或更高版本的以下 ASA 平台上安装运行版本 5.4.0.4 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

您仅可以在运行版本 9.3.2.2 的 ASA5506-X、ASA5506W-X、ASA5506H-X、ASA5508-X、ASA5516-X 和 ISA 3000 设备上安装运行版本 5.4.1.3 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-系列平台上运行适用于 Blue Coat X 系列的 Cisco NGIPS 版本 5.4.0.4 的。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

适用于 FireSIGHT 系统的 Web 界面版本 5.4.0.4 和版本 5.4.1.3 已在下表中列出的浏览器上进行了测试。

**说明：**如果您使用 Microsoft Internet Explorer 11 浏览器，则必须通过**工具 (Tools) > Internet 选项 (Internet Options) > 安全 (Security) > 自定义级别 (Custom level)** 禁用 Internet Explorer 设置中的**当将文件上传到服务器时包括本地目录路径 (Include local directory path when uploading files to server)** 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 40	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 <b>检查存储网页的较新版本</b> 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》中的“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》中的“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 后再安装其他版本。此过程可能需要数分钟。

要从 5.4.1 版映像更新为版本 5.4.0.4 或版本 5.4.1.3，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

## 安装更新

- 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 和 ASA5516-X)：

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 5.4.1.3，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 5.4.1 版或更高版本的防御中心更新至版本 5.4.1.3，将运行版本 5.4.1 或更高版本的具备 FirePOWER 服务的 Cisco ASA 更新至版本 5.4.1.3，以及将运行 FireSIGHT 系统版本 5.4 或更高版本的 ASA FirePOWER 模块和受管设备更新至版本 5.4.0.4，请参阅以下章节中所述的准则和步骤：

- [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 16 页](#)

**注意：**在更新期间不要重启或关闭设备，直至看登录提示。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，不需要您重新启动或关闭设备。

### 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

先更新防御中心，再更新其管理的设备。

### 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，则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。请确保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

在防御中心或受管设备上执行更新后，**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 5.4.1.3 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 5.4.1.3 更新，防御中心会重启。

**注意：**要将设备更新为版本 5.4.1.1，必须将 DC2000 和 DC4000 的 BIOS 更新为版本 2.0.1b。可从思科支持站点下载 BIOS 更新。CSCus10407

**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，不需要您重新启动或关闭设备。

**说明：**将防御中心更新至版本 5.4.1.3 会从设备中删除现有的卸载程序。

**说明：**如果您在启用了内联规范化的情况下将当前运行版本 5.3.x 的防御中心更新为版本 5.4，更新过程不会更改策略的行为。系统会根据需要添加用户层，以保留沿用的设置。

**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_升级-5.4.1.3-55.sh
```

**说明：**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**上传 (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。可以开始在任务队列 (**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” (Upgrade Status) 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. 审阅并接受《**最终用户许可协议 (EULA)**》。请注意，如果不接受 **EULA**，您将从设备注销。

12. 选择 **Help > About**，确认软件版本是否已正确列出：版本 5.4.1.3。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。

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。此时请勿自动应用已导入的规则。

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。**

要重新激活灰显的**应用 (Apply)** 按钮，请在设备配置中编辑任意界面，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 5.4.1.3 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

将防御中心更新为版本 5.4 版本 5.4.1 或版本 5.4.1.3 后，可以使用它们来更新其管理的设备。

防御中心必须运行版本 5.4 或更高版本，才能将其管理的设备更新至版本 5.4.1.3。由于虚拟受管设备没有网络界面，因此，您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 5.4.0.4 更新，所有设备都会重新启动，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 9 页。

**注意：**在更新受管设备前，请使用对其进行管理的防御中心将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，不需要您重新启动或关闭设备。

**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、ASA FirePOWER 模块和适用于 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：**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_升级-5.4.0.4-55.sh
```

- 对于系列 3 受管设备：

```
Sourcefire_3D_Device_S3_升级-5.4.0.4-55.sh
```

- 对于虚拟受管设备：

```
Sourcefire_3D_Device_Virtual64_VMware_升级-5.4.0.4-55.sh
```



## 安装更新

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

```
Sourcefire_3D_XOS_Device_升级-5.4.0.4-55.sh
```

- 对于 ASA FirePOWER 模块（555X-X-SSP-X 和 558X-X-SSP-X）：

```
Cisco_Network_Sensor_Upgrade-5.4.0.4-55.sh
```

- 对于 ASA FirePOWER 模块（ASA5506-X、ASA5506W-X、ASA5506H-X、5508-X、ASA5516-X 和 ISA 3000）：

```
Cisco_Network_Sensor_Upgrade-5.4.1.3-26.sh
```

4. 要将更新上传至防御中心，请选择 **系统 (System) > 更新 (Updates)**，然后点击“产品更新” (Product Updates) 选项卡中的 **上传更新 (Upload Update)**。浏览到更新并点击 **上传 (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。当在内联部署的适用于 Blue Coat X 系列的 Cisco NGIPS 设备上重新加载 VAP 时，流量将会中断。

**说明：**更新 X-系列设备时，必须等到设备重启并重新加载 VAP 完毕后，才能继续操作。

**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 5.4.0.4。

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：**要重新激活灰显的 **应用 (Apply)** 按钮，请在设备配置中编辑任意界面，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 5.4.0.4 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。**

## 已解决的问题

您可以使用 Cisco 漏洞搜索工具 (<https://tools.cisco.com/bugsearch/>) 跟踪此版本解决的缺陷。需要有 Cisco 帐户才能使用该工具。要查看更早期版本中解决的缺陷, 请访问传统说明跟踪系统。

### 版本 5.4.0.4 和版本 5.4.1.3 中已解决的问题:

- **安全问题**解决了一个 Linux 漏洞问题, 如 CVE-2011-4131 中所述。
- **安全问题**解决了受管设备在处理中断流量时遇到的微引擎故障问题。(CSCUu86214)
- 解决了以下问题: 无法将入侵策略重新应用到 (逐个或作为访问控制策略的一部分重新应用) 单台受管设备达到 4096 次或以上。(134385/CSCze89030)
- 解决了以下问题: 如果将其他策略引用的入侵策略导入为共享层或基本策略, 则入侵策略导入会失败。(144946/CSCze96151)
- 解决了以下问题: 系统在“入侵策略列表”页面上两次错误地列出已注册目标的数量。(CSCus08840)
- 解决了以下问题: 无法从剪贴板将旧事件添加到新突发事件, 即使“突发事件”页面的剪贴板部分中的事件显示为空白。(CSCus67128)
- 解决了以下问题: 如果您编辑具有多个类别条件的访问控制规则, 并尝试删除其中一个条件, 则系统只会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域为目标, 并执行 **show fastpath-rules** CLI 命令, 则系统会将入侵规则报告为非活动规则。(CSCut32479)
- 解决了以下问题: 在启用了**检查存档 (Inspect Archives)** 的情况下, 配置文件策略会导致 Snort 停止传输流量。(CSCut39253 和 CSCUu60621)
- 改善了故障排除。(CSCut43542)
- 提高了磁盘管理器的可靠性。(CSCut65740)
- 提高了关联规则性能。(CSCut97938)
- 解决了以下问题: 对以“Cisco”开头的 RPM 数据包管理器 (RPM) 文件进行降级不会正确重置 RPM 安装历史记录。(CSCut98525)
- 解决了以下问题: 如果将未经编辑的主动访问控制策略应用到 ASA FirePOWER 模块, 则策略应用会失败。(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: 长时间使用系统后, 与 AMP 云之间的连接可能会断开。(CSCUu24587)
- 解决了以下问题: 如果您在连接了 Cisco Nexus 7000 交换机的物理系列 3 设备上创建链路汇聚组 (LAG), 系统会遇到流量中断情况。(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: 在集群系列 3 设备上创建路由接口会导致连接问题。(CSCUu37668)
- 解决了以下问题: 如果您生成报告, 退出“报告模板” (Report Templates) 选项卡, 然后生成另一报告, 则“报告”页面的“报告模板” (Report Templates) 选项卡中的**发送邮件 (Send email)** 复选框不会保持选中状态。(CSCUu41580 和 CSCUu97750)
- 改进了对受监控主机数量的跟踪。(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, 则“访问控制策略” (Access Control Policy) 页面不会加载。(CSCUu83933)

## 已解决的问题

- 解决了以下问题：在极少数情况下，系统似乎不稳定，且无法从硬重置恢复。(CSCuu93154)
- 解决了以下问题：如果某些 DC4000 设备上出现驱动器故障，会导致 RAID 控制器故障以及数据丢失。(CSCuu93159)
- 解决了以下问题：即使有 URL 过滤许可证，产品许可控制面板构件也不会列出任何 URL 过滤许可证(CSCuu97762)
- 改进了 SFDatacorrelator 的性能(CSCuv48373)

## 早期版本中解决的问题

之前解决的问题按版本列出。

**版本 5.4.0.3 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**解决了跨站脚本 (XSS) 漏洞问题，如 CVE-2015-0707 中所述。
- **安全问题**解决了 Linux 及其他第三方的多个漏洞问题，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：如果 FirePOWER 7000 或 8000 系列受管设备检查出流量中存在格式不正确的数据包数据，系统可能会出现微引擎故障。(CSCuu10871 和 CSCuu26678)
- 如果路由是在系列 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，而且可以避免网络安全措施。(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：如果您从“对象管理”(Object Management) 页面中编辑了接口安全区，当堆栈设备配置不是最新版本时，它仍显示为最新版本。(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)
- 改进了多个控制面板构件。(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)

## 已解决的问题

- 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 SHA-256 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)
- 提高了 SFDataCorrelator 在处理过往邮件和 eStreamer 告警时的性能。(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)
- 解决了以下问题：系统在“网络文件轨迹”页面上显示不正确的文件类型信息。(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：在网络界面以及可通过外壳访问的日志文件中，系统在系统日志消息中暴露纯文本密码。(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：如果不重启 SFR5585-X 服务卡的情况下重启配置有大量子接口的 ASA5585-X 设备，则 SFR5585-X 服务卡将出现故障。(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 物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)

## 已解决的问题

- 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：当从“报告”(Report) 页面生成报告时，如果点击**中继主机 (Relay Host)** 可配置选项旁边的“编辑”(Edit) 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，该漏洞可使未经身份验证的远程攻击者利用 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) 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 和 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 和 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。请注意，运行版本 3.8.4 的 SSL 设备已解决了这个问题。()
- 解决了以下问题：如果应用引用了 URL 过滤许可证、安全情报许可证或为检查以下任何设备而配置的 SSL 策略的访问控制策略，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)

## 已解决的问题

- 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，该漏洞可使未经身份验证的远程攻击者通过 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，“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，当会话刷新时，系统会在“连接事件” (Connection Events) 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” (Intrusion Events) 表视图和“连接事件” (Connection Events) 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)
- 《FireSIGHT 系统用户指南》已进行了更新，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)
- 访问控制策略现在具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 和 144635/CSCze95200)
- 改进了生成报告时的磁盘管理器清理能力。(143933/CSCze94240 和 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：已解密的 SSL 会话将连接日志中的 URL 显示为 **http://** 而不是 **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 和 144544/CSCze95599)

## 已解决的问题

- 解决了以下问题：如果您为防御中心或受管设备的 **eth1** 启用 DHCP，则系统会错误地保存配置，为 **eth0** 和 **eth1** 都启用 DHCP。(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：如果在与 8000 系列受管设备连接的网络模块上创建链接汇聚组 (LAG) 接口，然后关闭设备，则删除网络模块将导致出现错误。(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 及其他第三方的多个漏洞问题，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)

## 已解决的问题

- 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)
- 现在您可以在受管设备的网络界面中，通过“管理接口”(Management Interface) 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：由启用了预处理程序选项的入侵规则生成的事件的系统日志警报消息是 **Snort Alert** 警报消息而不是自定义消息。(134270/CSCze88831)
- 解决了以下问题：如果在启用了**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”(Event View Settings) 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)



## 已解决的问题

- 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，且该报告包含以**文件名 (File Name)** 为 x 轴的图表，则系统不会在 x 轴文件名中显示 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 设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**最后修改日期**。(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：如果防御中心未向注册设备，且防御中心没有数据，则查看“入侵事件图表” (Intrusion Events Graph) 页面 (**概览 (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” (Scheduling) 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” (User Management) 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)

## 已知问题

- 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：系统提供的已保存的搜索 **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” (Connection Summary) 控制面板 (**概览 (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**，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，您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：如果防御中心将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”。(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：如果仅以 CSV 格式生成报告，则报告部分查询会忽略沿用时间窗口的选项。(143403/CSCze94376)
- 解决了以下问题：如果系统出现丢包情况，则 Modbus 预处理器无法生成事件。(142450/CSCze95921)
- 解决了以下问题：如果创建引用 SSL 策略的访问控制规则，且该 SSL 策略设置为用于解密流量，则策略应用会失败。(144518/CSCze94864)
- 解决了以下问题：如果创建入侵策略或网络分析策略并向其添加共享层，然后导出和导入新策略，则系统会生成**后端导入失败**错误，且不会导入策略。(144905/CSCze96093)

## 已知问题

版本 5.4.0.4 和版本 5.4.1.3 中报告了以下已知问题：

- 如果将包含用户组的访问控制策略应用到具备 Firepower 服务的 ASA 设备 (ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X 和 ASA5516-X)，则系统不会检测与应用的策略匹配的流量。对此的解决方法是，应用包含单个用户而非用户组的访问控制策略。(144428/CSCze95542)
- 如果您作为用户而非管理员用户登录到系统，并编辑所应用的入侵策略的基本层，则系统会错误地标记**管理员更新**的策略。(CSCur79437)
- 在某些情况下，如果在“用户首选项” (User Preferences) 页面的“时区偏好” (Time Zone Preference) 选项卡 (**管理 (Admin) > 用户首选项 (User Preferences) > 时区偏好 (Time Zone Preference)**) 中更改所选的时区，则系统可能不会纳入夏令时，且可能显示错误的时间。(CSCur92028)

## 已知问题

- 系统日志消息不填充以下字段的信息：HTTP 引用 (HTTP Referrer)、用户代理 (User Agent) 和引用的主机 (Referenced Host)。(CSCus18179)
- 在某些情况下，如果将思科 IOS 空路由实例添加到思科 IOS 补救措施，并启用密码以登录路由器，则设备不会启用密码，且补救措施会失败。对此的解决方法是，不启用密码。(CSCus45769)
- 如果应用引用安全情报 (SI) 对象的访问控制策略失败，请重新应用访问控制策略。如果仍无法应用策略，请联系支持部门。(CSCus50470)
- 在某些情况下，如果为 Nmap 模块设置扫描实例，远程操作系统检测可能无法正确识别检测到的操作系统的版本。对此的解决方法是，参阅正确操作系统的主机脚本输出。(CSCut23654)
- 在选中删除<设备名称>上的接口配置 (Remove the interface configurations on <device name>)选项的情况下，如果拆分包含 NAT 策略的设备集群，则拆分集群后在辅助设备上应用策略会失败。对此的解决方法是，在拆分集群设备时取消选中删除<设备名称>上的接口配置 (Remove the interface configurations on <device name>)。(CSCut98774)
- 如果在没有任何发现事件的防御中心上打开“发现统计信息” (Discovery Statistics) 页面 (概览 (Overview) > 摘要 (Summary) > 发现统计信息 (Discovery Statistics))，则系统会显示以下错误消息：错误 500：内部服务器错误。(CSCuu00749)
- 在某些情况下，如果创建文件策略和 NAT 策略，并启用带有 HTTP 端口号的 TCP 流预处理器规则，但该端口并非网络访问策略的 HTTP 预处理器配置页面上可用的端口，则系统不会检测与所配置文件策略操作匹配的流量中的恶意软件，并会异常地下载恶意软件内容。(CSCuu24472)
- 有时，如果在没有 FireSIGHT 许可证的情况下将 LDAP 组下载到防御中心，则下载 LDAP 用户或 LDAP 组会失败，且系统会生成以下错误：已达到用户数量限制。(CSCuu35615)
- 在某些情况下，如果至少启用了两个管理接口，当系统与其中一个接口断开连接时，系统会默认使用错误的网关 IP 地址，且该接口不可访问。(CSCuu44020)
- 在某些情况下，在带有集群接口的高可用性配置受管设备上，如果使用多个 Cisco 冗余协议 (SFRP) IP 地址在“设备管理”页面的“虚拟路由器” (Virtual Router) 选项卡中配置静态路由器、虚拟路由器或虚拟路由器过滤器，则系统可能会错误地禁用所配置的静态路由、虚拟路由器或虚拟路由器过滤器，且路由可能无法重新启用。(CSCuu47325)
- 有时，在具备 FirePOWER 服务的 Cisco ASA 配置为“失效打开”模式的情况下，如果 Snort 进程重新开始而不是允许未经检查的流量通过，则系统会丢弃流量。(CSCuu68273)
- 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)) 使用取反后的子网 IP 地址按原始客户端 IP 进行过滤，则系统会错误地排除没有原始客户端 IP 的入侵事件。(CSCuu68438)
- 在某些情况下，如果在“应用检测器” (Application Detectors) 页面 (策略 (Policies) > 应用检测器 (Application Detectors)) 的“用户第三方映射” (Third-Party Mapping) 部分中创建产品映射集并添加固定映射，则系统不会为“供应商”下拉菜单生成供应商列表。(CSCuu79373)
- 如果使用 MAC 地址配置主机输入主机，则系统会错误地存储 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)) 生成 MAC 地址字段。(CSCuu90757)
- 如果向防御中心注册了多台设备，则尝试连接 MySQL 可能会失败。(CSCuu94784)
- 在某些情况下，如果网络浏览器正被用于大容量媒体 (例如，视频流)，则系统在“摘要控制面板” (Summary Dashboard) (概览 (Overview) > 控制面板 (Dashboard) > 摘要控制面板 (Summary Dashboard)) 的“显示的主要 Web 应用”和“显示的主要客户端应用”构件中不会显示正确的字节数。(CSCuu97036)
- 为了优化流量检查，思科不建议再次检查 SSL 流量。(CSCuu97712)

## 已知问题

- 在某些情况下，如果创建具有交互拦截操作的访问控制规则，查看被拦截的网页，并选择**继续 (Continue)** 按钮以避开拦截，则系统可能会将页面从 http:// 地址重定向到 https:// 地址，且网页不会重新加载。(CSCUu97946)
- 如果某用户属于包含 LDAP 用户感知对象的组，但该组在 Active Directory 服务器上设置为主用户组，则该用户不会包含在从 Active Directory 服务器下载的访问受控用户列表中，且该用户不能添加到访问控制规则。(CSCUv03821)
- 在某些情况下，如果从模板生成连接事件报告并修改**最大结果数 (Maximum Results)** 值，则系统不会保存新的最大结果数值，而是用默认值生成报告。(CSCUv06557)
- 在某些情况下，如果创建虚拟路由器过滤器，系统会将虚拟路由器 OSPF 路径类型错误地保存为 **Ext-2** 而非 **Ext-1**。(CSCUv08158)
- 在某些情况下，如果将系统策略配置为使用远程 NTP 服务器，以便与使用注册的 ASA 5500-X 设备、系列 2 设备或运行低于版本 5.4 的系列 3 设备的系统实现时间同步，当遇到闰秒问题时，系统可能会占用大量 CPU。(CSCUv11738)
- 在某些情况下，如果创建具有交互拦截操作的访问控制规则，用 Chrome 网络浏览器查看被拦截的网页时，选择**继续 (Continue)** 按钮无法避开页面拦截。对此的解决方法是，使用 Firefox 或 Internet Explorer 查看被拦截的网页。(CSCUv21748)
- 在某些情况下，在添加集群并编辑接口时无法编辑辅助接口，且系统会生成以下错误：**无法加载容器**。(CSCUv25142)
- 系统允许保存大于 4095 的整数 VLAN 标记，但 VLAN 标记应限制为介于 0 至 4095 之间的整数。系统仅匹配介于 0 至 4095 之间的整数 VLAN 标记。(CSCUv25963)
- 如果在“对象管理”(Object Management) 页面 (**对象 (Objects) > 对象管理 (Object Management) > PKI**) 生成新的内部 CA 证书，生成的证书的有效期限仅为 30 天 (有效期限应为 10 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，则 IOC 仍会显示在“按主机列出的危害表现”控制面板构件中。(CSCUv41376)
- 如果创建 SSL 规则来检测端口值大于或等于 **32768** 的端口上的流量，则系统不会检测与该 SSL 规则中指定的端口值匹配的流量。(CSCUv44860)
- 如果访问控制策略包含超过可用端口范围内存的极大端口范围，则策略应用会失败。对此的解决方法是，缩小在访问控制策略中引用的端口范围，然后重新应用策略。(CSCUv64114)
- 系统不包含未映射至主机 IP 地址的新用户帐户，且配置为按组检测用户流量的分组访问控制规则会失败。(CSCUv78458)
- 在某些情况下，如果在创建访问控制规则时选择所有国家/地区作为目标国家/地区或源国家/地区，则系统不会匹配 IPv6 流量。对此的解决方法是，在创建访问控制规则时选择单个国家/地区作为目标国家/地区或源国家/地区。(CSCUv93913)
- 在某些情况下，如果在设备上配置静态路由，并重新应用系统策略，则系统会错误地删除静态路由。(CSCUw07826)
- 在某些情况下，SFDataCorrelator 会遇到问题，无法正确地处理 Snort 消息。(CSCUw34423)

早期版本中报告了以下已知问题：

- 在某些情况下，如果在客户端传输文件时进行 Microsoft Windows 更新，则无法检测到传输的文件，因为客户端通过不同的会话将文件分成多个部分进行传输，而系统无法重组这些部分来检测完整的文件。(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)
- 在某些情况下，如果创建 SSL 规则并启用日志记录，则“连接事件”(Connection Events) 页面 (**分析 (Analysis) > 连接 (Connections) > 事件 (Events)**) 不会显示 URL 类别或 URL 信誉值。(142878/CSCze93434)

## 已知问题

- 如果新建报告（**概览 (Overview) > 报告 (Reporting) > 报告模板 (Report Templates)**），并在使用 Internet Explorer 11 查看网络界面时尝试插入报告参数，则报告参数不会添加到报告部分描述中。对此的解决方法是，使用 Internet Explorer 10。(142950/CSCze94011)
- 有时，如果在通过 ASA 会话命令登录的情况下尝试使用 **SFR system restart** CLI 命令，设备可能会停止进程，且不会重新开始这些进程。这个问题影响到除 ASA5506-X 以外的所有设备。(143135/CSCze94403)
- 在某些情况下，如果创建具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“连接开始”和“连接结束”日志记录，则系统会因为**用户旁路**而不记录“连接开始”事件。(143357/CSCze93672、144167/CSCze94675)
- 在某些情况下，如果集群系列 3 设备进入维护模式后遇到电源故障，重启设备并不能使系统恢复正常。如果设备无法从维护模式成功恢复，请联系支持部门。(143504/CSCze94928)
- 如果创建的访问控制规则设置为允许引用设置为**解密放弃 (Decrypt-Resign)** 的 SSL 规则以及设置为“内联模式下丢弃”的入侵规则的流量，则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，访问控制策略似乎已过时，但事实并非如此。(14412/CSCze95029)
- 在某些情况下，如果将引用两个入侵策略的同一个访问控制策略应用到两台设备，编辑第一个入侵策略，然后将编辑过的策略重新应用到第一台设备，并将这两台设备组成集群，则修改过的入侵策略会在第二台设备上被标记为“已过时”。对此的解决方法是，将同样引用这两个入侵策略的另一个访问控制策略应用到第二台设备。(144136/CSCze95126)
- 在某些情况下，如果创建引用规则的访问控制策略，且引用的规则带有设置了“交互拦截”操作的 HTTP 响应页面，那么，当您尝试访问会生成 HTTP 响应页面的 URL 时，您将无法在同一个浏览器的其他选项卡中访问相同的网页。(144419/CSCze95694)
- 在某些情况下，系统在“连接事件” (Connection Events) 表视图（**分析 (Analysis) > 连接 (Connections) > 事件 (Events)**）中可能不显示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，系统在“发现统计信息” (Discovery Statistics) 页面（**概览 (Overview) > 摘要 (Summary) > 发现统计信息 (Discovery Statistics)**）上统计信息摘要的以下行中不显示任何事件：**事件总数 (Total Events)**、**最后一小时的事件总数 (Total Events Last Hour)** 和**最后一天的事件总数 (Total Events Last Day)**。(145153/CSCze95751)
- 在某些情况下，如果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)**），并选择**最后一小时 (Last Hour)** 作为时间范围，则生成的图表为空，而非包含来自“入侵事件”表视图的数据。(145237/CSCze95774)
- 设备可能需要等待很长时间才能接通电源。(145248/CSCze96068)
- 在某些情况下，如果启用“失效打开” Cisco 冗余协议 (SFRP)，且该协议设置为仅在高可用性配置的 ASA 5515 模块上进行监控，那么，当设备遇到故障转移时，模块可能会异常地多次从主用模式转变为备用模式。(145256/CSCze95812)
- 如果使用网络地址转换配置运行版本 5.0 或更高版本的 ASA FirePOWER 模块，则系统会错误地处理与所应用的访问控制策略、入侵策略和网络发现策略匹配的数据信道。(145274/CSCze96017)
- 在某些情况下，如果在高可用性配置系统的“警报” (Alerts) 页面（**策略 (Policies) > 操作 (Actions) > 警报 (Alerts)**）的“高级恶意软件防护” (Advanced Malware Protections) 选项卡中进行更改，所做的更改可能无法在设备之间正确同步。(CSCur46711)
- 如果未禁用流量配置文件便删除它，则系统会允许已删除的配置文件继续使用资源而不会产生流量。(CSCur48345)

## 已知问题

- 在某些情况下，如果使用思科冗余协议 (SFRP) 配置系列 3 受管设备集群，并应用网络地址转换 (NAT) 规则，则该集群的主设备和辅助设备都会响应在匹配的流量中检测到的地址解析协议 (ARP)，但正常情况下应该只有主设备作出响应。对此的解决方法是，在创建集群设备的 NAT 规则时，将主设备的 SFRP 接口指定为主接口，将辅助设备的 SFRP 接口指定为备用接口。(CSCur55568)
- 如果创建预定任务以在防御中心上安装新版本的漏洞数据库 (VDB)，那么，即使已安装了最新的 VDB 版本，系统也不会发出告警，且每次安排该任务时防御中心都会从主用模式切换到备用模式。Cisco 不建议启用自动 VDB 更新。(CSCur59252)
- 如果在 81xx 子系列设备上配置入侵策略中的 DNS 预处理器时使用无效的 IP 地址，系统功能可能会成倍地减慢。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对，**show traffic-statistics** CLI 命令不会显示该内联接口对中第二个接口的数据。(CSCur59771)
- 在某些情况下，对于可能已过期或可能已从注册的设备删除的许可证，“设备管理” (Device Management) 页面 (**设备 (Devices) > 设备管理 (Device Management)**) 的“设备” (Device) 选项卡显示为**是**，但正常情况下应显示为**否**。(CSCur61884)
- 在某些情况下，如果从“许可证” (Licenses) 页面 (**系统 (System) > 许可证 (Licenses)**) 删除保护许可证，则系统不会按预期递减已使用的许可证数量。对此的解决方法是，从“设备管理” (Device Management) 页面 (**设备 (Devices) > 设备管理 (Device Management)**) 禁用许可证。(CSCur61927)
- 无法应用当前应用的访问控制策略中未引用的现有入侵策略。(CSCur72904)
- 如果有匹配的解压缩数据或非分块数据，那么，即使在 ASA5506-X 设备上检测到入侵情况，系统也不会生成有关用 gzip 压缩的 HTTP 流量或分块的 HTTP 响应数据的告警。(CSCur77397)
- 在某些情况下，如果系统在策略应用过程中丢失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)**) 会显示**应用到设备 (apply to devices)**。对此的解决方法是，编辑并重新应用网络发现策略。(CSCur81583)
- 如果创建的入侵策略引用设置为**忽略音频/视频数据信道 (Ignore Audio/Video Data Channel)** 的网络分析策略，则系统会异常地生成有关会话初始协议 (SIP) 音频数据的告警。(CSCur83184)
- 如果将防御中心或受管设备的时间手动配置为过去的时间，则“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)**) 不会显示告警。(CSCur85894)
- 在某些情况下，如果将集群系列 3 受管设备的路由器接口配置为使用私有 IP 地址和 Cisco 冗余协议 (SFRP) IP 地址，则系统无法识别哪个 IP 地址是主地址，且不会建立开放最短路径优先 (OSPF) 连接。(CSCur86355)
- 在某些情况下，如果在启用了 HTTP 预处理器和**无限解压缩 (Unlimited Decompression)** 时创建网络分析策略，且有入侵规则设置为针对用 gzip 压缩的 HTTP 流量中的数据发出告警，则系统可能不会针对与应用的入侵规则匹配、超过 65535 字节解压缩数据的流量生成告警。(CSCur87659)
- 在某些情况下，如果部署大型数据库，并尝试在防御中心上创建故障排除文件，则系统会利用外部内存来执行该任务，并会生成以下错误：**内存不足! (Out of memory!)**。(CSCur97450)
- 如果要更新为版本 5.4.1.1 或更高版本的 DC2000 和 DC4000 设备运行的不是 BIOS 版本 2.0.1b，则更新会失败。如果由于防御中心运行较低版本的 BIOS 而导致更新失败，请联系支持部门。(CSCus10407)
- 检测 Sametime 应用时可能会出现误报。(CSCus17165)
- 您在 ASA5585-X 设备上不能重置管理员用户的密码。(CSCus17991)
- 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，则危害表现 (IOC) 可能无法从 IOC 表视图 (**分析 (Analysis) > 主机 (Hosts) > 危害表现 (Indications of Compromise)**) 删除或解析。(CSCus24116)

## 已知问题

- 在某些情况下，如果应用的 SSL 策略中引用了单个受信任的证书颁发机构 (CA) 组或对象，则系统不允许从该策略删除这个组或对象。对此的解决方法是，向策略添加其他 CA 组或对象，并从当前 SSL 策略删除受信任的 CA 组或对象。(CSCus42239)
- 如果运行版本 5.4.1 的 ASA5506-X 设备上未安装 URL 许可证，或者许可证不可用，则“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 过滤更新消息。(CSCus51935)
- 在某些情况下，如果创建单独 URL 对象并将其添加到 URL 组对象，然后修改这个组对象，则单独对象的工具提示不会反映组对象的更新值。(CSCus51943)
- 有时，如果在 URL 许可证不可用或已删除的情况下尝试添加新的 URL 许可证，则“云服务”(Cloud Services) 页面 (**系统 (System) > 本地 (Local) > 配置 (Configuration)**) 的启用自动更新 (**Enable Automatic Updates**) 选项默认为不选中，但正常情况下应默认为选中。(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，那么，无论入侵策略是在规则更新之前还是之后存在，系统都会错误地生成以下消息：**入侵策略已过时**。(CSCus59479)
- 有时，如果访问控制策略包含带有 **::/0** 的源地址和目标地址，则在仅应允许 IPv6 流量的情况下，“连接事件”表视图 (**分析 (Analysis) > 连接 (Connections) > 事件 (Events)**) 会包含 IPv4 和 IPv6 流量生成的事件。(CSCus63549)
- 如果您无法通过授权代理连接云，但可以通过直接连接进行连接，请联系支持部门。(CSCus83379)
- 在某些情况下，如果从防御中心将访问控制策略应用到 ASA5506-X，且该策略与启用了许多规则的多个入侵策略关联，则策略应用会失败。对此的解决方法是，减少使用的策略。入侵策略与变量集的每个唯一组合都算作一个策略，与访问控制策略关联的网络访问策略也算作一个策略。(CSCus95519)
- 解决了以下问题：如果在启用了动态分析的情况下创建包含文件策略的访问控制策略，当配置的代理端口是端口 80 时，将会无法连接综合安全情报云来进行动态分析。(CSCut01361)
- 在某些情况下，如果防御中心的数据库遇到系统问题，请确认已应用包含访问控制规则的访问控制策略。如果您发现缺少访问控制策略或规则，请联系支持部门。(CSCut30047)
- “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) 选项卡不包含已注册的 ASA55X5 或 ASA55X5-SSP-XX 设备作为选项。(CSCut41338)
- 在某些情况下，如果应用引用之前已删除的网络对象或组的访问控制规则，高可用性配置的防御中心不会意识到该网络对象或组已被删除，且会遇到问题。对此的解决方法是，删除包含已删除对象或组的规则，使用对象重新创建规则，然后应用策略。(CSCut54187)
- 在某些情况下，如果创建引用大量 LDAP 组的访问控制规则，且这些组包含访问受控用户，则系统会遇到延迟，且可能不会将流量与规则进行匹配。对此的解决方法是，限制在 LDAP 连接中配置的访问受限组数量。(CSCut56233)
- 对于在集群系列 3 设备上配置的虚拟路由器接口，系统不支持多个标准 IP 地址。(CSCut58601)
- 在某些情况下，如果更新高可用性配置的一对防御中心，则辅助防御中心的访问控制策略似乎可能是最新状态，而主防御中心的访问控制策略则不是。请注意，系统应报告访问控制策略引用的对象和策略的正确状态。(CSCut63260)
- 在某些情况下，如果为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，则系统会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是重复的，则 SFDatacorrelator 会遇到问题。如果遇到 SFDatacorrelator 性能问题，请联系支持部门。(CSCut65738)
- 在某些情况下，如果系统连续两次遇到故障，那么，即使未配置旁路模式，系统仍可能会进入旁路模式而不是尝试从第二次故障恢复，且流量可能会通过而不被检测出。(CSCut80892)

## 已知问题

- 使用 Chrome 浏览器时，如果尝试在“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)**) 选择所有应用过滤器，具体做法是，首先选择第一个可用的应用过滤器，然后按住 Shift 键并点击最后一个可用的应用过滤器，那么，只有选定的那两个应用过滤器处于选中状态。要包括所有可用的过滤器，必须逐一选择应用。(CSCut86012)
- 如果将以下具备 FirePOWER 服务的 Cisco ASA 从版本 5.4.1 更新为版本 5.4.1.1，FirePOWER 在更新过程中将会不可用：ASA5506-X、ASA506H-X、ASA5506W-X、ASA5508-X 和 ASA5516-X。更新设备后，FirePOWER 服务便可用。对此的解决方法是，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，在更新完成后在 ASA 模块上重启自适应安全设备管理器 (ASDM)。(CSCut89599)
- 在某些情况下，如果为内部部署配置的传感接口在系统重启时出现故障，则 Snort 会不断重启。(CSCut93464)
- 在某些情况下，如果在带有已注册设备的系统上启用配置的多个接口，并在该设备上使用 `show managers` CLI 命令，则系统会显示错误的 IP 地址。(CSCut95947)
- 在某些情况下，3D8xx 可能会遇到错误并丢失控制信道和信息信道。(CSCut98395)
- 如果在更新设备后遇到系统问题（例如，无法访问设备），请联系支持部门。(CSCuu01055)
- 如果在使用 `system support run-rule-profiling` CLI 命令时出现堆栈轨迹，请重新应用访问控制策略。(CSCuu02211)
- 在某些情况下，如果您禁用引用入侵策略的访问控制规则，在访问控制策略成功重新应用后，“访问控制” (Access Control) 页面 (**策略 (Policies) > 访问控制 (Access Control)**) 会将入侵策略错误地显示为过时状态。“入侵策略” (Intrusion Policy) 页面 (**策略 (Policies) > 入侵 (Intrusion) > 入侵策略 (Intrusion Policy)**) 会显示正确的策略状态。(CSCuu15483)
- 在某些情况下，如果创建包含地理位置条件的访问控制策略，流量将会无法按预期与该条件匹配。(CSCuu48800)
- “文件轨迹” (File Trajectory) 页面 (**分析 (Analysis) > 文件 (Files) > 网络文件轨迹 (Network File Trajectory)**) 将带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，而非显示为红色图标。(CSCuu17950)
- 在某些情况下，如果向防御中心注册 ASA FirePOWER 模块并重启 ASA FirePOWER 模块，则防御中心与虚拟 ASA 设备上 VMware 工具之间的数据信道连接会中断。对此的解决方法是，重新注册 ASA 设备。(CSCuu18450)
- 在某些情况下，如果备份某个防御中心，将备份还原到另一个防御中心，那么，您将无法登录到带有已还原备份的防御中心。如果在还原备份后无法登录到防御中心，请联系支持部门。(CSCuu35238)
- 从“设备管理” (Device Management) 页面的“接口” (Interfaces) 选项卡 (**设备 (Device) > 设备管理 (Device Management) > 接口 (Interfaces)**) 添加或编辑路由 IP 地址时，思科冗余协议 (SFRP) 播发间隔值似乎可编辑，即使实际上不可编辑。(CSCuu37687)
- 在某些情况下，如果向防御中心注册设备，然后更新注册的设备，那么，使用 `configure manager <IP address> add` CLI 命令会禁止防御中心管理注册的设备。对此的解决方法是，等待设备在更新后自动注册到防御中心。(CSCuu44265)
- 在某些情况下，如果在设备上使用 `system file copy` CLI 命令，可能无法退出 CLI 提示符。对此的解决方法是，使用 `ctr+c` 使命令退回到提示符。(CSCuu48793)
- 在某些情况下，如果系统长时间积聚大量流量，可能会导致延迟和流量中断。(CSCuu52545)
- 在某些情况下，如果为 3D8250 设备添加多个许可证，为 3D8260 设备或同属这个子系列的其他设备添加一个许可证，那么，在查看“许可证” (License) 页面 (**系统 (System) > 许可证 (Licenses)**) 时，系统会错误地列出最新加载了许可证的设备下的所有许可证。即使“许可证”页面错误地列出非预期设备的许可证，许可证仍可正确地应用。(CSCuu99789)
- 如果创建的备份具有包含空格的文件名，则无法将备份应用到防御中心。对此的解决方法是，使备份文件名不包含空格。(CSCuu99818)



## 获取帮助

- 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)**) 删除安全区，而 ASA5500-X 系列设备的已应用访问控制策略中引用了该安全区，那么，系统不会保存更改，且安全区无法删除。对此的解决方法是，从访问控制策略删除安全区，然后从“安全区”页面删除安全区。(CSCuv40232)
- 在“捕获的文件摘要” (Captured File Summary) 工作流程的表视图 (**分析 (Analysis) > 文件 (Files) > 捕获的文件 (Captured Files)**) 中，如果点击包含扩展字符的文件名，会出现内部服务器错误。(CSCuv40941)
- 如果在没有任何发现事件的防御中心上打开“发现统计信息” (Discovery Statistics) 页面 (**概览 (Overview) > 摘要 (Summary) > 发现统计信息 (Discovery Statistics)**)，会出现内部服务器错误。(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 支持站点，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](mailto: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>。

订阅《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。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请转至此 URL：[www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks)。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1110R)

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

© 2015 年 Cisco Systems, Inc. 保留所有权利。

♻️ 本文档使用含 10% 用后废料的再生纸在美国印制出版。

[获取帮助](#)