Cisco ASDM 7.5 (x) 版本说明

首次发布日期：2015 年 8 月 31 日
最后更新日期： 2016 年 1 月 28 日

本文档包含思科 ASA 系列思科 ASDM 7.5 (x) 版本信息。

重要说明

- 弃用电邮代理命令 ASA – 9.5 (2) 版本中已不再支持邮件代理命令（**imap4s**、**pop3s**、**smtps**）和子命令。
- 弃用 Select AAA 命令 ASA – 9.5 (2) 版本中已不再支持 AAA 命令和子命令（**override-account-disable**、**authentication crack**）。
- 弃用或迁移 CSD 命令 ASA – 9.5 (2) 版本中已不再支持 CSD 命令（**csd image**、**show webvpn csd image**、**show webvpn csd**、**show webvpn csd hostscan**、**show webvpn csd hostscan image**）。

  以下 CSD 命令将迁移：**csd enable** 迁移到 **hostscan enable**；**csd hostscan image** 迁移到 **hostscan image**。

新增功能

ASA 9.5(2.200)/ASDM 7.5(2.153) 新增功能

发布日期：2016 年 1 月 28 日

下表列出了 ASA 9.5(2.200) 版本/ASDM 7.5(2.153) 版本新增功能。

注意：此版本仅支持 ASAv。

表 1 ASA 9.5(2.200) 版本/ASDM 7.5(2.153) 版本新增功能

功能	说明
平台功能	
提供 Microsoft Azure 支持	标准 D3 虚拟机可支持 ASAv10。
许可功能	
ASAv 永久许可证保留	在不允许与 Cisco Smart Software Manager 之间进行通信的高安全性环境中，您可以请求提供 ASAv 永久许可证。 我们引入了以下命令：**license smart reservation**、**license smart reservation cancel**、**license smart reservation install**、**license smart reservation request universal**、**license smart reservation return** 无 ASDM 支持。
智能代理升级至 v1.6	智能代理从 1.1 版本升级到 1.6 版本。此升级支持永久许可证保留，同时也支持依据许可证账号中的权限集设置强加密 (3DES/AES) 许可证授权。 **注意：**如果您从 9.5(2.200) 版本降级，ASAv 将不保留许可注册状态。您需使用 **license smart register idtoken** *id_token* **force** 命令重新注册 (对于 ASDM，请查看**配置 (Configuration) > 设备管理 (Device Management) > 许可 (Licensing) > 智能许可 (Smart Licensing)** 页面，并使用 **Force registration** 选项；从 Smart Software Manager 中获取 ID 令牌。 我们未修改任何菜单项。

ASDM 7.5 (2.153) 新增功能

发布日期：2016 年 1 月 21 日

此版本中无新增功能。

ASA 9.5(2.1)/ASDM 7.5(2) 新增功能

发布日期：2015 年 12 月 14 日

下表列出了 ASA 9.5(2.1) 版本/ASDM 7.5(2) 版本新增功能。

注意：此版本仅支持 FirePOWER 9300 ASA 安全模块。

表 2 ASA 9.5(2.1) 版本/ASDM 7.5(2) 版本新增功能

功能	说明
平台功能	
为 Firepower 9300 ASA 安全模块提供 VPN 支持	您可使用 FXOS 1.1.3 版本配置 VPN 功能。
防火墙功能	
Firepower 9300 ASA 安全模块的流量卸载	您可以识别需从 ASA 中卸载并直接在 NIC 中切换的流量。该功能可提升数据中心的大数据流性能。 同时也需要 Firepower 可扩展操作系统 1.1.3 版本。 我们添加或修改了以下菜单项：**配置 (Configuration) > 防火墙 (Firewall) > 高级 (Advanced) > 卸载引擎 (Offload Engine)** 以及在 **配置 (Configuration) > 防火墙 (Firewall) > 服务策略规则 (Service Policy Rules)** 下添加或编辑规则时使用的**规则操作 (Rule Actions) > 连接设置 (Connection Settings)** 选项卡
高可用性功能	
支持 6 个模块机箱内集群，FirePOWER 9300 ASA 安全模块站点间集群	现在您可利用 FXOS 1.1.3 启用机箱内集群，并扩展至站点间集群。在最多 6 个机箱中最多可以包含 6 个模块。 我们未修改任何菜单项。
许可功能	
支持自动应用 FirePOWER 9300 ASA 安全模块的强加密 (3DES) 许可证	对于一般的 Cisco Smart Software Manager 用户，当他们在 Firepower 9300 上应用注册令牌时，只要符合相应条件，系统会自动启用强加密许可证。 **注意：**如果您通过 Smart Software Manager 卫星部署使用 ASDM 和其他强加密功能，您必须在部署 ASA 之后使用 ASA CLI 启用强加密 (3DES) 许可证。 此功能要求具有 FXOS 1.1.3 版本。 我们修改了以下菜单项：**配置 (Configuration) > 设备管理 (Device Management) > 许可 (Licensing) > 智能许可证 (Smart License)**

ASA 9.5(2)/ASDM 7.5(2) 新增功能

发布日期：2015 年 11 月 30 日

下表列出了 ASA 9.5(2) 版本/ASDM 7.5(2) 版本新增功能。

表 3 ASA 9.5(2) 版本/ASDM 7.5(2) 版本新增功能

功能	说明
平台功能	
提供 Cisco ISA 3000 支持	Cisco ISA 3000 是一个装有 DIN 导轨的坚固型工业安全设备。它是一种低功耗、无风扇设备，并配有千兆以太网和专用管理端口。该型号设备中预装了 ASA Firepower 模块。该型号的特殊功能包括自定义的透明模式默认配置，以及允许流量在出现功率损耗时继续通过设备的硬件旁路功能。 我们引入了以下菜单项：**配置 (Configuration) > 设备管理 (Device Management) > 硬件旁路 (Hardware Bypass)** *同样适用于 9.4.(1.225) 版本。*
防火墙功能	
DCERPC 检测改进和 UUID 过滤	DCERPC 检测现在支持 OxidResolver ServerAlive2 opnum5 消息的 NAT。现在您可根据 DCERPC 消息通用唯一标识 (UUID) 进行过滤，以便重置或记录特定消息类型。新 DCERPC 检测类映射可用于 UUID 过滤。 我们引入了以下菜单项：**配置 (Configuration) > 防火墙 (Firewall) > 对象 (Objects) > 类图 (Class Maps) > DCERPC**。我们修改了以下菜单项：**配置 (Configuration) > 防火墙 (Firewall) > 对象 (Objects) > 检测图 (Inspect Maps) > DCERPC**
Diameter 检测	现在您可以检测 Diameter 流量。Diameter 检测需要运营商许可证。 我们添加或修改了以下菜单项：**配置 (Configuration) > 防火墙 (Firewall) > 对象 (Objects) > 检测图 (Inspect Maps) > Diameter 和 Diameter AVP (Diameter** and **Diameter AVP)**；**配置 (Configuration) > 防火墙 (Firewall) > 服务策略 (Service Policy)** 中添加/编辑向导中的 **规则操作 (Rule Action) > 协议检测 (Protocol Inspection)** 选项卡
SCTP 检测和访问控制	现在您可以在服务对象、访问控制列表 (ACL) 和访问规则中使用 SCTP 协议和端口规范，并检测 SCTP 流量。SCTP 检测和访问控制需要运营商许可证。 我们添加或修改了以下菜单项：**配置 (Configuration) > 防火墙 (Firewall) > 访问规则 (Access Rules)** 添加/编辑对话框；**配置 (Configuration) > 防火墙 (Firewall) > 高级 (Advanced) > ACL Manager** 添加/编辑对话框；**配置 (Configuration) > 防火墙 (Firewall) > 高级 (Advanced) > Global Timeouts**；**配置 (Configuration) > 防火墙 (Firewall) > NAT**、添加/编辑静态网络对象 NAT 规则、**高级 NAT 设置 (Advanced NAT Settings)** 对话框；**配置 (Configuration) > 防火墙 (Firewall) > 对象 (Objects) > 服务对象/组 (Service Objects/Groups)** 添加/编辑对话框；**配置 (Configuration) > 防火墙 (Firewall) > 对象 (Objects) > 检测图 (Inspect Maps) > SCTP**；**配置 (Configuration) > 防火墙 (Firewall) > 服务策略 (Service Policy)** 添加/编辑向导中的 **规则操作 (Rule Action) > 协议检测 (Protocol Inspection)** 选项卡
现在支持在故障切换和 ASA 集群中增强运营商级 NAT	对于运营商级或大规模 PAT，您可以为每台主机分配端口块，而无需通过 NAT 一次分配一个端口转换（请参阅 RFC 6888）。现在支持在故障切换和 ASA 集群部署中使用此功能。 我们未修改任何菜单项。

表 3 ASA 9.5(2) 版本/ASDM 7.5(2) 版本新增功能（续）

功能	说明
可配置级别集群跟踪条目	默认情况下，所有级别的集群事件都储存在跟踪缓冲区中，包括大量低级事件。要将跟踪事件级别限制为更高级别，您可以设置集群跟踪事件的最低级别。 我们未修改任何菜单项。
ASA FirePOWER 6.0 中使用强制网络门户的主动身份验证	从 ASA FirePOWER 6.0 开始，要使用身份策略启用主动身份验证，需使用强制网络门户功能。 我们引入或修改了以下命令：**captive-portal**、**clear configure captive-portal**、**show running-config captive-portal**
高可用性功能	
站点间流移动性的 LISP 检测	思科定位编号分离协议 (LISP) 架构将设备身份与设备位置分离开，并分隔到两个不同的编号空间，使服务器迁移对客户端透明化。ASA 可以通过检测 LISP 流量确定位置更改，并使用此信息进行无缝集群操作；ASA 集群成员检查第一跳路由器与出口隧道路由器 (ETR) 或入口隧道路由器 (ITR) 之间的 LISP 流量，然后将流所有者位置更改为新站点。 我们引入或修改了以下菜单项： **配置 (Configuration) > 设备管理 (Device Management) > 高可用性和可扩展性 (High Availability and Scalability) > ASA 集群 (ASA Cluster) > 集群配置 (Cluster Configuration)** **配置 (Configuration) > 防火墙 (Firewall) > 对象 (Objects) > 检测图 (Inspect Maps) > LISP** **配置 (Configuration) > 防火墙 (Firewall) > 服务策略规则 (Service Policy Rules) > 协议检测 (Protocol Inspection)** **配置 (Configuration) > 防火墙 (Firewall) > 服务策略规则 (Service Policy Rules) > 集群 (Cluster)**
ASA 5516-X 支持集群	ASA 5516-X 现在支持由 2 台设备组成的集群。默认情况下，基本许可证中启用 2 台设备的集群。 我们未修改任何菜单项。
路由功能	
为组播路由提供 PIM 自举路由器 (BSR) 支持	目前，ASA 支持配置静态 RP，为不同的组路由组播流量。ASA 现在支持在包含多个 RP 的大型复杂网络中使用 PIM BSR 进行动态 RP 选择，以支持 RP 移动性。 我们引入了以下菜单项：**配置 (Configuration) > 设备设置 (Device Setup) > 路由 (Routing) > 组播 (Multicast) > PIM > 自举路由器 (Bootstrap Router)**
接口功能	
支持将辅助 VLAN 映射到主 VLAN	现在您可以为一个子接口配置一个或多个辅助 VLAN。当 ASA 接收到辅助 VLAN 的流量时，它会将流量映射到主 VLAN。 我们修改了以下菜单项： **配置 (Configuration) > 设备设置 (Device Setup) > 接口设置 (Interface Settings) > 接口 (Interfaces)** **配置 (Configuration) > 设备设置 (Device Setup) > 接口设置 (Interface Settings) > 接口 (Interfaces) > 添加接口 (Add Interface) > 通用 (General)**

表 3 ASA 9.5(2) 版本/ASDM 7.5(2) 版本新增功能（续）

功能	说明
远程接入功能	
支持多情景模式下的远程接入 VPN	现在您可在多情景模式中使用以下远程接入功能： ■ AnyConnect 3.x 及更高版本 （仅支持 SSL VPN ；无 IKEv2 支持） ■ 集中式 AnyConnect 映像配置 ■ AnyConnect 映像升级 ■ 对 AnyConnect 连接进行情景资源管理 **注意：**多情景模式下需要 AnyConnect Apex 许可证；您无法使用默认或传统许可证。 我们修改了以下菜单项：**配置 (Configuration) > 情景管理 (Context Management) > 资源级别 (Resource Class) > 添加资源级别 (Add Resource Class)**
无客户端 SSL VPN 提供基于 SAML 2.0 的单点登录 (SSO) 功能	ASA 充当 SAML 服务提供商。
无客户端 SSL VPN 条件调试	您可以根据过滤条件集进行过滤，以达到调试日志的目的，也可以更好地对其进行分析。
默认情况下，无客户端 SSL VPN 为禁用状态	无客户端 SSL VPN 缓存现在默认为禁用状态。禁用无客户端 SSL VPN 缓存可提供更强的稳定性。若要启用缓存，您必须手动操作。 我们修改了以下菜单项：**配置 (Configuration) > 远程接入 VPN (Remote Access VPN) > 无客户端 SSL VPN 接入 (Clientless SSL VPN Access) > 高级 (Advanced) > 内容缓存 (Content Cache)**
许可功能	
如果服务器证书的颁发层次结构出现更改，思科智能报障服务 (Smart Call Home)/智能许可 (Smart Licensing) 证书需进行验证	智能许可使用 Smart Call Home 基础设施。当 ASA 首次在后台配置智能报障服务的匿名报告时，它会自动创建一个信任点，这个信任点包含颁发过智能报障服务证书的 CA 的证书。ASA 现在支持在服务器证书颁发层次结构出现变更时对证书进行验证；您可以按一定时间间隔定期启用 trustpool 捆绑的自动更新功能。 我们修改了以下菜单项：**配置 (Configuration) > 远程接入 VPN (Remote Access VPN) > 证书管理 (Certificate Management) > 可信任证书池 (Trusted Certificate Pool) > 编辑策略 (Edit Policy)**
新运营商许可证	用于替换现有的 GTP/GPRS 许可证的新运营商许可证提供的支持包括 SCTP 和 Diameter 检测。对于 FirePOWER 9300 ASA 安全模块，**feature mobile-sp** 命令将自动迁移至 **feature carrier** 命令。 我们修改了以下菜单项：**配置 (Configuration) > 设备管理 (Device Management) > 许可 (Licensing) > 智能许可证 (Smart License)**
监控功能	
logging debug-trace 持久性	以前，当您启用 logging debug-trace 将调试重定向至系统日志服务器时，如果 SSH 连接中断（由于网络连接性问题或超时），调试进程将被清除。现在，只要 logging 命令有效，调试过程将持续。 我们未修改任何菜单项。

ASA 9.4(2.145)/ASDM 7.5(1.112) 新增功能

发布日期：2015 年 11 月 13 日

此版本中无新增功能。

注意：此版本仅支持 FirePOWER 9300 ASA 安全模块。

ASA 9.5(1.5)/ASDM 7.5(1.112) 新增功能

发布日期：2015 年 11 月 11 日

下表列出了 ASA 9.5(1.5) 版本/ASDM 7.5(1.112) 版本新增功能。

表 4 ASA 9.5(1.5) 版本/ASDM 7.5(1.112) 版本新增功能

功能	说明
平台功能	
支持 ASA FirePOWER 6.0	所有以前支持过的设备型号都支持 ASA FirePOWER 6.0 版本。
从 5512-X 到 5585-X 系列都支持通过 ASDM 管理 ASA FirePOWER 模块	在模块上运行 6.0 版本时，您可以使用 ASDM 来管理 ASA FirePOWER 模块，而无需使用 Firepower 管理中心 (Firepower Management Center)（以前称为 FireSIGHT 管理中心 (FireSIGHT Management Center)）来进行管理。运行 6.0 版本时，您还可以使用 ASDM 来管理 5506-X、5506H-X、5506W-X、5508-X 和 5516-X 上的模块。 无新增菜单项或命令。

ASDM 7.5 (1.90) 新增功能

发布日期：2015 年 10 月 15 日

下表列出了 ASDM 7.5(1.90) 版本新增功能。

表 5 ASDM 7.5(1.90) 版本新增功能

功能	说明
远程接入功能	
支持 AnyConnect 4.2 版本	ASDM 可支持 AnyConnect 4.2 版本及网络可视性模块 (NVM)。NVM 可提升企业管理员执行容量和服务规划、审计、合规性和安全分析的能力。NVM 收集终端遥测数据，在系统日志中记录流数据和文件信誉，并导出流记录给收集器（第三方供应商），由其执行文件分析并提供 UI 接口。 我们修改了以下菜单项：**配置 (Configuration) > 远程接入 VPN (Remote Access VPN) > 网络（客户端）接入 (Network (Client) Access) > AnyConnect 客户端配置文件 (AnyConnect Client Profile)** (一个名为**网络可视性服务配置文件 (Network Visibility Service Profile)** 的新文件)

ASA 9.4(2)/ASDM 7.5(1) 新增功能

发布日期：2015 年 9 月 24 日

此版本中无新增功能。

注意：此版本中不包含 ASAv 9.4(1.200) 功能。

注意：此版本不支持 ISA 3000。

ASA 9.4(1.225)/ASDM 7.5(1) 新增功能

发布日期：2015 年 9 月 17 日

下表中列出了思科 ISA 3000 9.4(1.225) 版本/ASDM 7.5(1) 版本中 ASA 的新增功能。

注意：此版本仅支持 Cisco ISA 3000。

表 6 ISA 3000 9.4(1.225) 版本/ASDM 7.5(1) 版本中 ASA 新增功能

功能	说明
平台功能	
提供 Cisco ISA 3000 支持	Cisco ISA 3000 是一个装有 DIN 导轨的坚固型工业安全设备。它是一种低功耗、无风扇设备，并配有千兆以太网和专用管理端口。该型号设备中预装了 ASA Firepower 模块。该型号的特殊功能包括自定义的透明模式默认配置，以及允许流量在出现功率损耗时继续通过设备的硬件旁路功能。 我们修改了以下菜单项：**配置 (Configuration) > 设备管理 (Device Management) > 硬件旁路 (Hardware Bypass)** **hardware-bypass boot-delay** 命令不适用于 ASDM 7.5(1) 版本。 *此功能不适用于 9.5(1) 版本。*

ASA 9.5(1.200)/ASDM 7.5(1) 新增功能

发布日期：2015 年 8 月 31 日

下表中列出了 ASA 9.5(1.200) 版本/ASDM 7.5(1) 版本新增功能。

注意：此版本仅支持 ASAv。

表 7 ASA 9.5(1.200) 版本/ASDM 7.5(1) 版本新增功能

功能	说明
平台功能	
提供 Microsoft Hyper-V 管理引擎支持	扩展 ASAv 虚拟机监控程序配置文件。
支持 ASAv5 低内存	ASAv5 现在只需要 1 GB RAM 即可运行。而此前它需要 2 GB 的内存。对于已部署的 ASAv5s，您应将分配的内存减少至 1 GB，若不进行此操作，系统将显示错误消息提示您使用的内存已超出许可范围。

ASA 9.5(1)/ASDM 7.5(1) 新增功能

注意：新增的、更改的和已弃用的系统日志消息将列在系统日志消息指南中。

发布日期：2015 年 8 月 12 日

下表中列出了 ASA 9.5(1) 版本/ASDM 7.5(1) 版本新增功能。

注意：此版本不支持 Firepower 9300 ASA 安全模块或 ISA 3000。

表 8 ASA 9.5(1) 版本/ASDM 7.5(1) 版本新增功能

功能	说明
防火墙功能	
GTPv2 检测及对 GTPv0/1 检测的改进	GTP 检测现在可以处理 GTPv2。此外，所有版本的 GTP 检测现在均支持 IPv6 地址。 我们修改了以下菜单项：**配置 (Configuration) > 防火墙 (Firewall) > 对象 (Objects) > 检测图 (Inspect Maps) > GTP**
对 IP 选项检测的改进	IP 选项检测现在支持所有可能的 IP 选项。您可以对检测进行调整以允许、清除或丢弃任何标准的或试验性选项，包括尚未定义的选项。还可以为 IP 选项检测图中尚未明确定义的选项设置默认行为。 我们修改了以下菜单项：**配置 (Configuration) > 防火墙 (Firewall) > 对象 (Objects) > 检测图 (Inspect Maps) > IP 选项 (IP Options)**
对运营商级 NAT 的改进	对于运营商级或大规模 PAT，您可以为每台主机分配端口块，而无需通过 NAT 一次分配一个端口转换（请参阅 RFC 6888）。 我们引入了以下菜单项：**配置 (Configuration) > 防火墙 (Firewall) > 高级 (Advanced) > PAT 端口块分配 (PAT Port Block Allocation)**。我们添加了对象 NAT **启用端口块分配 (Enable Block Allocation)** 并两次添加了 NAT 对话框。
高可用性功能	
为路由防火墙模式下的 Spanned EtherChannel 提供站点间集群支持	现在您可以在路由防火墙模式下对 Spanned EtherChannel 使用站点间集群。要避免 MAC 地址摆动，请为每个集群成员配置一个站点 ID，这样就可在站点的设备间共享每个接口的站点特定 MAC 地址。 我们修改了以下菜单项：**配置 (Configuration) > 设备管理 (Device Management) > 高可用性和可扩展性 (High Availability and Scalability) > ASA 集群 (ASA Cluster) > 集群配置 (Cluster Configuration)**
自定义接口或集群控制链路发生故障时的 ASA 集群自动重新加入行为	现在您可以自定义接口或集群控制链路发生故障时的自动重新加入行为。 我们修改了以下菜单项：**配置 (Configuration) > 设备管理 (Device Management) > 高可用性和可扩展性 (High Availability and Scalability) > ASA 集群 (ASA Cluster) > 自动重新加入 (Auto Rejoin)**
ASA 集群支持 GTPv1 和 GTPv2	ASA 集群现在支持 GTPv1 和 GTPv2 检测。 我们未修改任何菜单项。
TCP 连接的集群复制延迟	该功能可以延迟导向器/备份流的创建，从而避免与短期流量相关的“不必要的工作”。 我们修改了以下菜单项：**配置 (Configuration) > 设备管理 (Device Management) > 高可用性和可扩展性 (High Availability and Scalability) > ASA 集群复制 (ASA Cluster Replication)** *同样适用于 Firepower 9300 ASA 安全模块 9.4(1.152) 版本。*

表 8 ASA 9.5(1) 版本/ASDM 7.5(1) 版本新增功能（续）

功能	说明
禁用 ASA 集群中硬件模块的健康状况监控	默认情况下，当使用集群时，ASA 会监控已安装的硬件模块（例如 ASA FirePOWER 模块）的运行状况。如果您不希望硬件模块故障触发故障切换，您可以禁用模块监控。 我们修改了以下菜单项：**配置 (Configuration) > 设备管理 (Device Management) > 高可用性和可扩展性 (High Availability and Scalability) > ASA 集群 (ASA Cluster) > 集群接口健康状况监控 (Cluster Interface Health Monitoring)**
在 ASA 5506H 上启用管理 1/1 接口作为故障切换链路	现在您只能在 ASA 5506H 上将管理 1/1 接口配置为故障切换链路。此功能允许您使用设备上的所有其他接口作为数据接口。说明：如果您使用了此功能，便不能使用 ASA Firepower 模块，因为它要求管理 1/1 接口仍作为常规管理接口。 我们修改了以下菜单项：**配置 (Configuration) > 设备管理 (Device Management) > 高可用性和可扩展性 (High Availability and Scalability) > 故障切换 (Failover) > 设置 (Setup)**
路由功能	
支持 IPv6 策略型路由	策略型路由现在支持 IPv6 地址。 我们修改了以下菜单项： **配置 (Configuration) > 设备设置 (Device Setup) > 路由 (Routing) > 路由图 (Route Maps) > 添加路由图 (Add Route Map) > 策略型路由 (Policy Based Routing)** **配置 (Configuration) > 设备设置 (Device Setup) > 路由 (Routing) > 路由图 (Route Maps) > 添加路由图 (Add Route Maps) > 匹配子句 (Match Clause)**
为策略型路由提供 VXLAN 支持	现在您可以在 VNI 接口中启用策略型路由。 我们修改了以下菜单项：**配置 (Configuration) > 设备设置 (Device Setup) > 接口设置 (Interface Settings) > 接口 (Interfaces) > 添加/编辑接口 (Add/Edit Interface) > 通用 (General)**
为身份防火墙和 Cisco Trustsec 提供策略型路由支持	您可以先配置身份防火墙和 Cisco TrustSec，然后再在策略型路由的路由图中使用身份防火墙和 Cisco TrustSec ACL。 我们修改了以下菜单项：**配置 (Configuration) > 设备设置 (Device Setup) > 路由 (Routing) > 路由图 (Route Maps) > 添加路由图 (Add Route Maps) > 匹配子句 (Match Clause)**
仅用于管理的接口的独立路由表	ASA 现在支持为仅用于管理的接口使用独立的路由表，从而将管理流量与数据流量分隔开。 我们未修改任何菜单项。
支持协议无关组播 - 源特定组播 (PIM-SSM) 直接通过	ASA 现允许 PIM-SSM 数据包在您启用组播路由后直接通过，但有一种情况除外：ASA 是最后一跳路由器时。此功能使得在选择组播组时更加灵活，同时也防止了多种攻击；主机只接收明确请求的数据源发来的流量。 我们未修改任何菜单项。
远程接入功能	
IPv6 VLAN 映射	经改进后，ASA VPN 代码现已支持所有 IPv6 功能。管理员不需要更改配置。
提供无客户端 SSL VPN SharePoint 2013 支持	为此 SharePoint 新版本增加了支持和一个预定义的应用模板。 我们修改了以下菜单项：**配置 (Configuration) > 远程接入 VPN (Remote Access VPN) > 无客户端 SSL VPN 接入 (Clientless SSL VPN Access) > 门户 (Portal) > 书签 (Bookmarks) > 添加书签列表 (Add Bookmark List) > 选择书签类型 (Select Bookmark Type) > 预定义应用模板 (Predefined application templates)**

表 8 ASA 9.5(1) 版本/ASDM 7.5(1) 版本新增功能（续）

功能	说明
无客户端 VPN 动态书签	我们将 CSCO_WEBVPN_DYNAMIC_URL 和 CSCO_WEBVPN_MACROLIST 添加到使用书签时的宏列表中。管理员可利用这些宏配置出可在无客户端用户的门户中生成多个书签链接的单个书签，并静态配置多个书签来利用 LDAP 属性地图提供的大小随机的列表。 我们修改了以下菜单项：**配置 (Configuration) > 远程接入 VPN (Remote Access VPN) > 无客户端 SSL VPN 接入 (Clientless SSL VPN Access) > 门户 (Portal) > 书签 (Bookmarks)**
VPN 标志长度增加	登录后在 VPN 远程客户端门户上显示的整体标志长度已从 500 增至 4000。 我们修改了以下菜单项：**配置 (Configuration) > 远程接入 VPN (Remote Access VPN) > .... 添加/编辑内部组策略 (Internal Group Policy) > 通用参数 (General Parameters) > 标志 (Banner)**
ASA 5506-X、5506W-X、5506H-X 和 5508-X 上的 Cisco Easy VPN 客户端	此版本支持在 ASA 5506-X 系列和 ASA 5508-X 型号的设备上使用 Cisco Easy VPN。当连接到 VPN 头端时，ASA 会充当 VPN 硬件客户端。当一个 ASA 设备连接到 Easy VPN 端口，其下面连接的所有设备（计算机、打印机等）都可通过 VPN 进行通信；这些设备无需单独运行 VPN 客户端。请注意只有一个 ASA 接口可用作 Easy VPN 端口；要使多个设备连接到该端口，您需在该端口安置一个第二层交换机，再将您的设备连接至交换机。 我们引入了以下菜单项：**配置 (Configuration) > VPN > Easy VPN Remote**
监控功能	
在系统日志消息中显示无效用户名	您现在可以在失败登录尝试的系统日志消息中显示无效用户名。在默认情况下，如果用户名无效或者有效性未知时，用户名会被隐藏。例如当用户意外键入密码而不是用户名时，在生成的系统日志消息中隐藏“用户名”会更为安全。您可能希望利用显示的无效用户名对登录问题进行故障排除。 我们修改了以下菜单项：**配置 (Configuration) > 设备管理 (Device Management) > 日志记录 (Logging) > 系统日志设置 (Syslog Setup)** *此功能同样适用于 9.2(4) 和 9.3(3) 版本。*
REST API 功能	
REST API 1.21 版本	我们增加了对 REST API 1.2.1 版本的支持。

系统要求

ASDM 客户端操作系统和浏览器要求

下表中列出了推荐使用的、受 ASDM 支持的客户端操作系统和 Java。

表 9 操作系统和浏览器要求

操作系统	浏览器				Java SE 插件
	Internet Explorer	Firefox	Safari	Chrome	
Microsoft Windows（英文版和日文版）： 8 7 Server 2008 Server 2012	是	是	不支持	是	7.0 或更高版本
Apple OS X 10.4 及更高版本	不支持	是	是	是（仅限 64 位版本）	7.0 或更高版本
Red Hat Enterprise Linux 5（GNOME 或 KDE）： 桌面版 带工作站选项的桌面版	不适用	是	不适用	是	7.0 或更高版本

Java 和浏览器兼容性

下表列出了 Java、ASDM 和浏览器兼容性的兼容性警告。

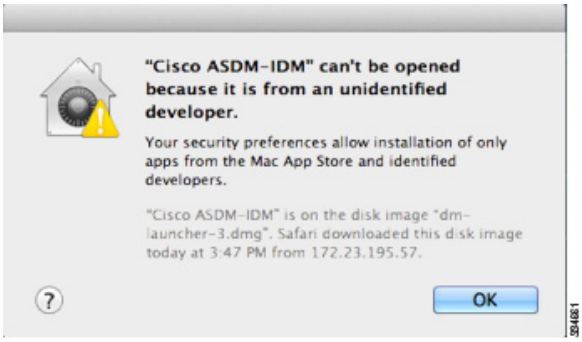
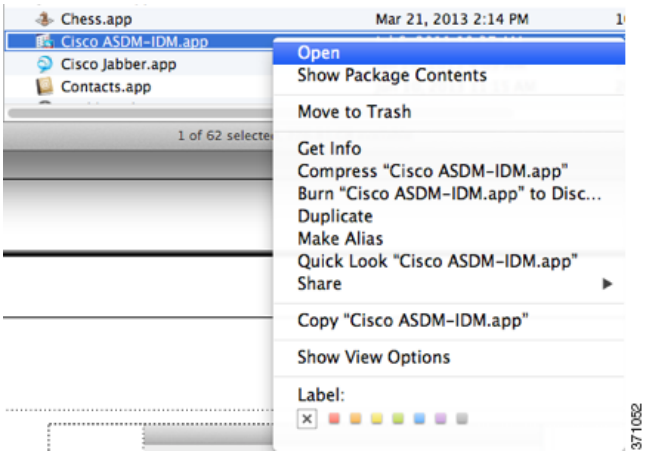
表 10 Java 与 ASDM 兼容性相关注意事项

Java 版本	条件	说明
7 Update 51	ASDM Launcher 需要可信任证书	要继续使用 Launcher，请执行以下其中一项操作： ■ 将 Java 升级到 Java 8 或降级到 Java 7 update 45 或更低版本。 ■ 在 ASA 上安装由已知 CA 颁发的可信任证书。 ■ 安装自签证书并使用 Java 进行注册。请参阅为 ASDM 安装身份证书。 ■ 或者，使用 Java Web Start。 **注意：**Java 7 update 51 不支持 ASDM 7.1(5) 及更低版本。如果您已升级 Java，并且无法再启动 ASDM 以将其升级到 7.2 版本或更高版本，则可以使用 CLI 升级 ASDM，也可以在 Java 控制面板中为每个要使用 ASDM 管理的 ASA 添加安全性异常。请参阅“解决方法”一节，网址： http://java.com/en/download/help/java_blocked.xml 添加安全性异常后，启动旧版本 ASDM，然后升级到 7.2 或更高版本。
	在极少数情况下，使用 Java Web Start 时无法加载在线帮助	在极少数情况下，启动在线帮助时，浏览器视窗会加载，但内容无法显示。浏览器报告以下错误：“Unable to connect”。 解决方法： ■ 使用 ASDM Launcher 或： ■ 清除 Java 运行时参数中的 **-Djava.net.preferIPv6Addresses=true** 参数： a. 启动 Java 控制面板。 b. 点击 **Java** 选项卡。 c. 点击 **View**。 d. 清除以下参数：**-Djava.net.preferIPv6Addresses=true** e. 点击 **OK**，然后点击 **Apply**，再次点击 **OK**。
7 Update 45	使用不可信任证书时，ASDM 将显示一条有关缺失“权限”属性的黄色警告	由于 Java 中存在的一个漏洞，因此，如果没有在 ASA 上安装可信任证书，您将会在 JAR 清单中看到指示缺少权限属性的黄色警告。**可忽略此警告**；ASDM 7.2 或更高版本包含“权限”(Permission) 属性。为了防止出现该警告，请安装可信任证书（由已知 CA 颁发）；或者依次选择**配置 (Configuration) > 设备管理 (Device Management) > 证书 (Certificates) > 身份证书 (Identity Certificates)** 以在 ASA 上生成自签证书。启动 ASDM，当出现证书警告时，选中 **Always trust connections to websites** 复选框。
7	ASA 需要有强加密许可证 (3DES/AES)	ASDM 需要一个与 ASA 的 SSL 连接。您可以向思科申请一个 3DES 许可证： 1. 前往 www.cisco.com/go/license。 2. 点击 **Continue to Product License Registration**。 3. 在许可门户中，点击文本字段旁边的 **Get Other Licenses**。 4. 从下拉列表中选择 **IPS、 Crypto、 Other...**。 5. 将 **ASA** 键入至 **Search by Keyword** 字段。 6. 在 **Product** 列表中选择 **Cisco ASA 3DES/AES License**，然后点击 **Next**。 7. 输入 ASA 的序列号，然后按照提示为 ASA 申请 3DES/AES 许可证。

表 10 Java 与 ASDM 兼容性相关注意事项（续）

Java 版本	条件	说明
全部	■ 自签证书或不可信任证书 ■ IPv6 ■ Firefox 和 Safari	如果 ASA 使用自签证书或不可信任证书，当使用 HTTPS 通过 IPv6 浏览时，Firefox 和 Safari 将无法添加安全性异常。请访问 https://bugzilla.mozilla.org/show_bug.cgi?id=633001。此警告会影响从 Firefox 或 Safari 到 ASA 的所有 SSL 连接（包括 ASDM 连接）。要避免此警告，请为 ASA 配置由可信任证书颁发机构颁发的正确证书。
	■ ASA 上的 SSL 加密必须包括 RC4-MD5 和 RC4-SHA1，*或者*在 Chrome 中禁用 SSL 虚假启动 ■ Chrome	如果更改 ASA 上的 SSL 加密以排除 RC4-MD5 和 RC4-SHA1 算法（默认情况下已启用这些算法），Chrome 将由于 Chrome“SSL 虚假启动”功能而无法启动 ASDM。我们建议重新启用其中一种算法（参阅**配置 (Configuration) > 设备管理 (Device Management) > 高级 (Advanced) > SSL 设置 (SSL Settings)** 窗格）；您也可以根据 Run Chromium with flags 使用 **--disable-ssl-false-start** 标签在 Chrome 中禁用 SSL 虚假启动。
	服务器专用 IE9	对于服务器专用 Internet Explorer 9.0，“不要将加密的页面保存到硬盘中 (Do not save encrypted pages to disk)”选项在默认情况下处于启用状态（请参阅工具(Tools) > 网络选项 (Internet Options) > 高级 (Advanced)）。此选项会导致初始 ASDM 下载失败。请务必禁用此选项以允许 ASDM 下载。
	OS X	在 OS X 上，第一次运行 ASDM 时，系统可能会提示您安装 Java。根据需要按照提示进行安装。安装完成后，ASDM 将启动。

表 10 Java 与 ASDM 兼容性相关注意事项（续）

Java 版本	条件	说明
全部	OS X 10.8 及更高版本	您需要允许 ASDM 运行，因为它未使用 Apple 开发人员 ID 进行签名。如果未更改安全首选项，将会出现一个错误窗口。  1. 要允许 ASDM 运行，请右键点击 （或按住 Ctrl 键并点击） **Cisco ASDM-IDM Launcher** 图标，然后选择 **Open**。  2. 随即将会出现一个类似的错误窗口，但您可以通过该窗口打开 ASDM。点击 **Open**，系统将打开 ASDM-IDM Launcher。 

为 ASDM 安装身份证书

使用 Java 7 update 51 及更高版本时，ASDM Launcher 需要可信任证书。满足证书要求的一个简单方法就是安装自签身份证书。可使用 Java Web Start 启动 ASDM，直到安装证书。

请参阅为 ASDM 安装身份证书中的说明在 ASA 上安装用于 ASDM 的自签名身份证书，以及通过 Java 注册证书。

增加 ASDM 配置内存

ASDM 最多支持 512 KB 的配置。如果超出此数量，可能会遇到性能问题。例如加载配置时，状态对话框显示已完成配置的百分比，但如果有大型配置，它将停止递增并显示为暂停操作，即使 ASDM 仍可能在处理配置。如果发生此情况，我们建议考虑增加 ASDM 系统堆内存。

增加 Windows 中的 ASDM 配置内存

要增加 ASDM 堆内存大小，请通过执行以下程序编辑 **run.bat** 文件。

程序

1. 转到 ASDM 安装目录，例如 C:\Program Files (x86)\Cisco Systems\ASDM。
2. 使用任意文本编辑器编辑 **run.bat** 文件。
3. 在以“start javaw.exe”开头的行中，更改前缀为“-Xmx”的参数以指定所需堆大小。例如，如需 768 MB 内存，请将参数更改为 -Xmx768M；如需 1 GB 内存，请将参数更改为 -Xmx1G。
4. 保存 **run.bat** 文件。

增加 Mac 操作系统中的 ASDM 配置内存

要增加 ASDM 堆内存大小，请通过执行以下程序编辑 **Info.plist** 文件。

程序

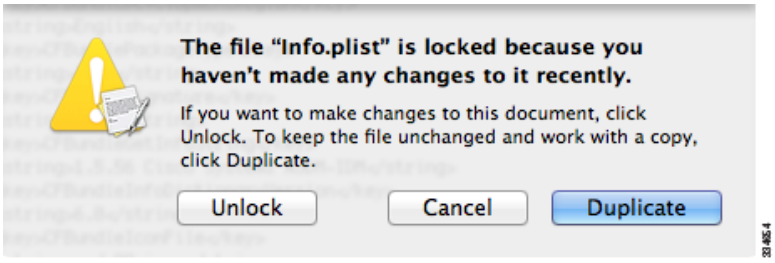
1. 右键点击 **Cisco ASDM-IDM** 图标，然后选择 **Show Package Contents**。
2. 在 **Contents** 文件夹中，双击 **Info.plist** 文件。如果已安装开发人员工具，该文件会在 **Property List Editor** 中打开。否则，它将在 **TextEdit** 中打开。
3. 在 **Java > VMOptions** 下方，更改前缀为“-Xmx”的字符串以指定所需堆大小。例如，如需 768 MB 内存，请将参数更改为 -Xmx768M；如需 1 GB 内存，请将参数更改为 -Xmx1G。

```
<key>CFBundleIconFile</key>
<string>asdm32.icns</string>

<key>VMOptions</key>
<string>-Xms64m -Xmx512m</string>


<key>CFBundleDocumentTypes</key>
  <array>
```

4. 如果该文件已锁定，则将看到如下错误：



5. 点击 **Unlock** 并保存文件。

   如果未看到 **Unlock** 对话框，请退出编辑器，右键点击 **Cisco ASDM-IDM** 图标，选择 **Copy Cisco ASDM-IDM**，并将其粘贴到您拥有写入权限的位置，例如桌面。然后从该副本中更改堆大小。

ASA 与 ASDM 兼容性

有关 ASA/ASDM 软件和硬件要求及兼容性信息（包括模块兼容性），请参阅思科 ASA 兼容性。

VPN 兼容性

有关 VPN 兼容性，请参阅支持的 VPN 平台和 Cisco ASA 5500 系列。

升级软件

请参阅下表以获取您的版本的升级路径。某些版本需要先进行临时升级，然后才能升级到最新版本。

注意：如果您从 9.5(2.200) 版本降级，ASAv 将不保留许可注册状态。您需使用 **license smart register idtoken** *id_token* **force** 命令重新注册 (对于 ASDM，请查看 **配置 (Configuration) > 设备管理 (Device Management) > 许可 (Licensing) > 智能许可 (Smart Licensing)** 页面，并使用 **Force registration** 选项)；从 Smart Software Manager 中获取 ID 令牌。

注意：除以下集群外，故障切换和 ASA 集群的零停机时间升级 (Zero Downtime Upgrades) 无特殊要求。

- 从 9.0(1) 升级至 9.1(1)(CSCue72961) - 不支持零停机时间升级。
- 升级至 9.5(2)(CSCuv82933) - 如果您在升级主设备之前输入 **show cluster info**，升级的从设备会显示“DEPUTY_BULK_SYNC”；其他不匹配的状态也会显示。您可以忽略此显示；当您升级完所有设备后，状态将正确显示。
- 从 9.5(2)(CSCuv82933) 降级 - 当从 9.5(2) 降级时，不支持零停机时间降级。您必须大致在同一时间重新加载所有设备，这样当设备恢复在线时可形成新的集群。如果您等待所有设备按顺序重新加载完，则无法形成集群。

当前 ASA 版本	首先升级到：	然后升级到：
8.2(x)	8.4(6)	9.5(1) 或更高版本
8.3(x)	8.4(6)	9.5(1) 或更高版本
8.4(1) 至 8.4(4)	8.4(6)、9.0(4) 或 9.1(2)	9.5(1) 或更高版本
8.4(5) 及更高版本	-	9.5(1) 或更高版本
8.5(1)	9.0(4) 或 9.1(2)	9.5(1) 或更高版本
8.6(1)	9.0(4) 或 9.1(2)	9.5(1) 或更高版本
9.0(1)	9.0(4) 或 9.1(2)	9.5(1) 或更高版本
9.0(2) 或更高版本	-	9.5(1) 或更高版本
9.1(1)	9.1(2)	9.5(1) 或更高版本
9.1(2) 或更高版本	-	9.5(1) 或更高版本
9.2(x)	-	9.5(1) 或更高版本
9.3(x)	-	9.5(1) 或更高版本
9.4(x)	-	9.5(1) 或更高版本

有关升级的详细步骤，请参阅 9.5 版本升级指南。

遗留和已解决漏洞

此版本的遗留和已解决漏洞可通过思科缺陷搜索工具查看。您可通过该基于 Web 的工具访问思科漏洞跟踪系统，在上面查看此产品和其他思科硬件和软件产品存在的缺陷和漏洞。

注意：您必须使用 Cisco.com 帐户才能登录并访问思科缺陷搜索工具。如果您没有 Cisco.com 帐户，您可以注册一个帐户。如果您没有思科支持合同，您只能通过 ID 查找漏洞，而无法使用搜索功能。

有关思科缺陷搜索工具的详细信息，请参阅缺陷搜索工具帮助及常见问题。

遗留漏洞

7.5(2.153) 版本中的遗留漏洞

如果您有思科支持合同，您可使用以下动态搜索查找 7.5(2.153) 版本中严重程度在 3 级及以上的所有漏洞：

- 搜索 7.5(2.153) 版本中的遗留漏洞。

下表列出了在发布此版本说明时存在的遗留漏洞。

表 11 ASA 7.5(2.153) 版本中的遗留漏洞

漏洞	说明
CSCux13150	ASDM：policy-map global_policy 无法使用备份/恢复功能
CSCux26490	如果超过 245 个字符，ASDM 将删除整个 DAP 书签列表
CSCux53184	MC：接口共享时无法更改为防火墙模式
CSCux59614	ASDM 从命令中移动 ACE 时会复制备注信息
CSCux63266	DAP 策略 - 从 HS3.x 升级到 HS4.x 时需升级 dap.xml
CSCux69363	ASDM 7.5(2) 密码存储显示为禁用

7.5(2) 版本中的遗留漏洞

如果您有思科支持合同，您可使用以下动态搜索查找 7.5(2) 版本中的所有遗留漏洞：

- 搜索 7.5(2) 版本中的遗留漏洞。

下表列出了在发布此版本说明时存在的遗留漏洞。

表 12 ASA 7.5(2) 版本中的遗留漏洞

漏洞	说明
CSCux11651	ASDM 无法删除 ACL 说明（备注）句段
CSCux13150	ASDM：policy-map global_policy 无法使用备份/恢复功能
CSCux26490	如果超过 245 个字符，ASDM 将删除整个 DAP 书签列表
CSCux33151	ASDM 复制而不是替换 ACL 中的备注信息

表 12 ASA 7.5(2) 版本中的遗留漏洞（续）

漏洞	说明
CSCux35016	加密图中 ASDM 的差异
CSCux37581	ASDM 7.5.2 不显示活跃的 Anyconnect 客户端
CSCux53184	MC：接口共享时无法更改为防火墙模式
CSCux59614	ASDM 从命令中移动 ACE 时会复制备注信息
CSCux63266	DAP 策略 - 从 HS3.x 升级到 HS4.x 时需升级 dap.xml
CSCux69363	ASDM 7.5(2) 密码存储显示为禁用

7.5(1.112) 版本中的遗留漏洞

如果您有思科支持合同，您可使用以下动态搜索查找 7.5(1.112) 版本中的所有遗留漏洞：

- 搜索 7.5(1.112) 版本中的遗留漏洞。

下表列出了在发布此版本说明时存在的遗留漏洞。

表 13 ASA 7.5(1.112) 版本中的遗留漏洞

漏洞	说明
CSCuv76021	ASDM Gtp 系统日志不匹配

7.5(1.90) 版本中的遗留漏洞

如果您有思科支持合同，您可使用以下动态搜索查找 7.5(1.90) 版本中的所有遗留漏洞：

- 搜索 7.5(1.90) 版本中的遗留漏洞。

下表列出了在发布此版本说明时存在的遗留漏洞。

表 14 ASA 7.5(1.90) 版本中的遗留漏洞

漏洞	说明
CSCuv76021	ASDM Gtp 系统日志不匹配

7.5(1) 版本中的遗留漏洞

如果您有思科支持合同，您可使用以下动态搜索查找 7.5(1) 版本中的所有遗留漏洞：

- 搜索 7.5(1) 版本中的遗留漏洞。

下表列出了在发布此版本说明时存在的遗留漏洞。

表 15 ASA 7.5(1) 版本中的遗留漏洞

漏洞	说明
CSCuv76021	ASDM Gtp 系统日志不匹配

已解决的漏洞

7.5 (2.153) 版本中已解决的漏洞

如果您有思科支持合同，请使用以下搜索查找已解决的漏洞：

- 搜索 7.5(2.153) 版本中已解决的漏洞。

下表列出了在发布此版本说明时已经解决的漏洞。

表 16 ASA 7.5(2.153) 版本中已解决的漏洞

漏洞	说明
CSCux11651	ASDM 无法删除 ACL 说明（备注）句段
CSCux33151	ASDM 复制而不是替换 ACL 中的备注信息
CSCux35016	加密图中 ASDM 的差异
CSCux37581	ASDM 7.5.2 不显示活跃的 Anyconnect 客户端

7.5(2) 版本中已解决的漏洞

如果您有思科支持合同，请使用以下搜索查找已解决的漏洞：

- 搜索 7.5(2) 版本中已解决的漏洞。

下表列出了在发布此版本说明时已经解决的漏洞。

表 17 ASA 7.5(2) 版本中已解决的漏洞

漏洞	说明
CSCuv00153	当访问 SNMP 配置节时的 ASDM NullPointerException
CSCuv20248	ASDM 7.4.x 无法打开设备
CSCuv50152	ASDM：当匹配任一流量时，向导配置错误的 DCD 选项
CSCuv66298	ASDM VPN 向导身份验证选项卡错误
CSCuv82314	无法在 Mac OS 上使用 ASDM 添加新的 DAP 策略
CSCuw02084	ASDM 在删除端口通道子接口时会发送两次删除指令
CSCuw08188	ASDM 将确切值推送至组策略，打破继承规则
CSCuw18046	ASDM：已创建组策略，但未与隧道组关联
CSCuw60507	ASDM 无法删除或修改 NAT 规则
CSCuw64395	ASDM DAP：需将 Windows 8.1 添加到终端操作系统属性列表
CSCuw83683	虽然 DfltGrpPolicy DTLS 压缩已被禁用，但在 ASDM 上似乎为启用状态

7.5(1.112) 版本中已解决的漏洞

如果您有思科支持合同，请使用以下搜索查找已解决的漏洞：

- 搜索 7.5(1.112) 版本中已解决的漏洞。

下表列出了在发布此版本说明时已经解决的漏洞。

表 18 ASA 7.5(1.112) 版本中已解决的漏洞

漏洞	说明
CSCuv20248	ASDM 7.4.x 无法打开设备

7.5(1.90) 版本中已解决的漏洞

如果您有思科支持合同，请使用以下搜索查找已解决的漏洞：

- 搜索 7.5(1.90) 版本中已解决的漏洞。

下表列出了在发布此版本说明时已经解决的漏洞。

表 19 ASA 7.5(1.90) 版本中已解决的漏洞

漏洞	说明
CSCut04399	升级至 Java 8 后，ASDM 保留在 MAC 上
CSCuv00153	当访问 SNMP 配置节时的 ASDM NullPointerException
CSCuv20248	ASDM 7.4.x 无法打开设备
CSCuw09242	无法配置 2 个以上的使用 ASDM 7.5.1 的 ASA 接口

7.5(1) 版本中已解决的漏洞

如果您有思科支持合同，请使用以下搜索查找已解决的漏洞：

- 搜索 7.5(1) 版本中已解决的漏洞。

最终用户许可证协议

有关最终用户许可证协议的信息，请访问 http://www.cisco.com/go/warranty。

相关文档

有关 ASA 的更多信息，请参阅思科 ASA 系列文档导航。

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。