思科 ASDM 7.7(x) 版本说明

首次发布日期: 2017 年 01 月 23 日

上次修改日期: 2017 年 03 月 09 日

思科 ASDM 7.7(x) 版本说明

本文档包含用于思科 ASA 系列的思科 ASDM 版本 7.7(x) 的版本信息。

重要说明

- 在扩展/高压环境下，AnyConnect 远程访问 VPN IPv6 DTLS 隧道可能会导致 ASA 回溯（例如：拥有大量隧道或隧道不断连接 ASA 头端或与之断开)。**解决方法**：使用 IPv6 AnyConnect IKEv2 或 IPv4 AnyConnect DTLS VPN 远程访问会话类型。(CSCvc77123)
- ASA 9.x 中使用的 RSA 工具套件版本与 ASA 8.4 使用的版本不同，导致两个版本之间的 PKI 行为不同。

  例如，运行 9.x 软件的 ASA 允许使用长度为 73 个字符的“组织名称值 (OU)”(Organizational Name Value (OU) 字段导入证书。运行 8.4 软件的 ASA 允许使用 60 个字符的 OU 字段名称导入证书。因为存在差异，所以 ASA 9.x 中可以导入的证书在 ASA 8.4 中则无法导入。如果您试图将 ASA 9.x 证书导入运行版本 8.4 的 ASA，可能会收到错误“错误：导入 PKCS12 操作失败”。

系统要求

本节列出了运行此版本的系统要求。

ASDM 客户端操作系统和浏览器要求

下表列出支持的建议用于 ASDM 的客户端操作系统和 Java。

表 *1*：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）： 10 8 7 Server 2012 R2 Server 2012 Server 2008	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 与浏览器的兼容性

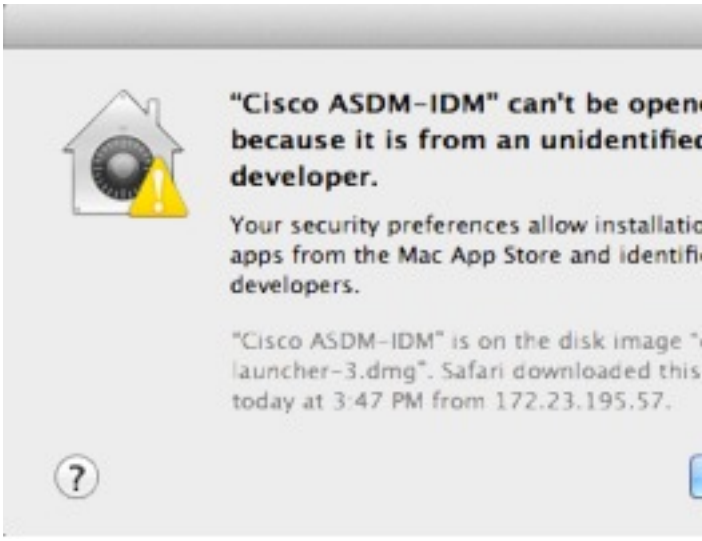
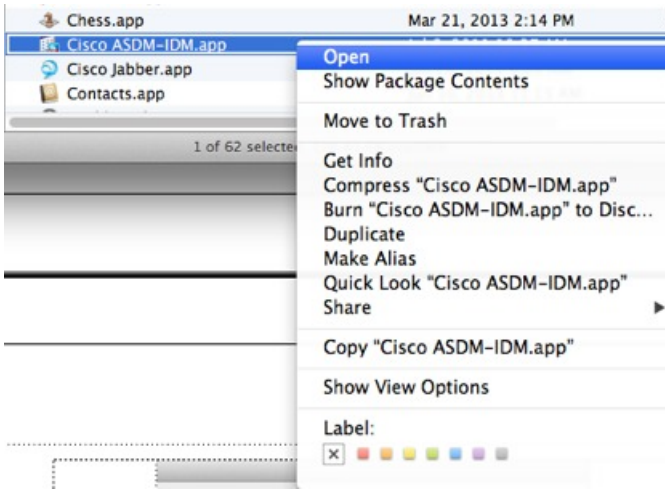
下表列出了 Java、ASDM 和浏览器兼容性的兼容性警告。

Java 版本	条件	备注
7 Update 51	ASDM Launcher 需要可信证书	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 上安装来自已知 CA 的可信证书。 • 安装自签证书并使用 Java 进行注册。请参阅安装用于 ASDM 的身份证书。 • 另外也可以使用 Java Web Start。 **注释** 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，浏览器窗口会加载，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： 1 启动 Java 控制面板。 2 点击 **Java** 选项卡。 3 点击 **View**。 4 清除此参数：**-Djava.net.preferIPv6Addresses=true** 5 点击 **OK**，然后点击 **Apply**，再次点击 **OK**。

Java 版本	条件	备注
7 Update 45	使用不可信证书时，ASDM 将显示一条有关缺失“权限”属性的黄色警告	由于 Java 中存在漏洞，如果 ASA 上未安装可信证书，您会看到一条黄色警告，表示 JAR 证明中缺失“权限”属性。**可忽略此警告**；ASDM 7.2 或更高版本包含“权限”属性。为了防止显示警告，请按照可信证书（来自已知 CA）；或在 ASA 上选择**配置 (Configuration)** > **设备管理 (Device Management)** > **证书 (Certificates)** > **身份证书 (Identity Certificates)** 生成一个自签证书。启动 ASDM，当显示证书警告时，选中**始终信任网站连接 (Always trust connections to websites)** 复选框。
7	ASA 上需要安全性高的加密许可证 (3DES/AES)	ASDM 需要 SSL 连接至 ASA。您可以向思科申请一个 3DES 许可证： 1 转到 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**获取其他许可证 (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，并按照提示为 ASA 申请 3DES/AES 许可证。

Java 版本	条件	备注
全部	• 自签证书或不可信证书 • IPv6 • Firefox 和 Safari	如果 ASA 使用自签证书或不可信证书，在使用 HTTPS 通过 IPv6 浏览时，Firefox 和 Safari 则无法添加安全特例。请参阅 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）。为了避免此警告，请为ASA配置一个由可信证书颁发机构签发的正确证书。
	• 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。我们建议您重新启用这些算法之一（请参阅**配置 (Configuration)** > **设备管理 (Device Management)** > **高级 (Advanced)** > **SSL 设置 (SSL Settings)** 面板）；或者可以在 Chrome 中使用 **--disable-ssl-false-start** 标记根据使用标记运行 Chromium 禁用 SSL 虚假启动。
	服务器专用 IE9	对于服务器中的 Internet Explorer 9.0，默认情况下**“不将加密的页面保存到磁盘 (Do not save encrypted pages to disk)”**选项处于启用状态（请参阅**工具 (Tools)** > **Internet 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。

Java 版本	条件	备注
全部	OS X 10.8 及更高版本	

Java 版本	条件	备注
		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，将会出现一个错误屏幕。  1 要使 ASDM 运行，请右击（按住 Ctrl 点击）思科 ASDM-IDM 启动程序图标，然后选择**打开 (Open)**。  2 随即将会出现一个类似的错误屏幕；但您可以通过该屏幕打开 ASDM。点击 **Open**。系统将打开 ASDM-IDM Launcher。

Java 版本	条件	备注
		

为 ASDM 安装身份证书

使用 Java 7 update 51 及更高版本时，ASDM 启动程序需要可信证书。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。

请参阅安装用于 ASDM 的身份证书在 ASA 上安装适用于 ASDM 的自签名身份证书，并在 Java 中注册该证书。

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。

步骤 1 转到 ASDM 安装目录，例如 C:\Program Files (x86)\Cisco Systems\ASDM。

步骤 2 使用任意文本编辑器编辑 **run.bat** 文件。

步骤 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。

步骤 4 保存 **run.bat** 文件。

增加 Mac OS 中的 ASDM 配置内存

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

步骤 1 右键点击 **Cisco ASDM-IDM** 图标，然后选择 **Show Package Contents**。

步骤 2 双击**内容 (Contents)** 文件夹中的 **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。

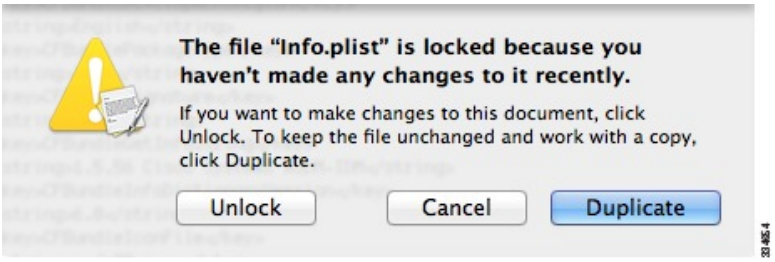
步骤 3 在 **Java** > **VMOptions** 下，更改前缀“-Xmx”的字符串以指定所需的堆大小。例如，如需 768 MB 内存，请将参数更改为 -Xmx768M；如需 1 GB 内存，请将参数更改为 -Xmx1G。

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

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


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

步骤 4 如果该文件已锁定，则将看到如下错误：



步骤 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。然后从该副本更改堆大小。

ASA 与 ASDM 的兼容性

有关 ASA/ASDM 软硬件要求及兼容性的信息（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，请参阅思科 ASA 5500 系列支持的 VPN 平台。

新功能

本节列出了每个版本的新功能。

注释 有关新增、更改和弃用的系统日志消息，请参阅系统日志消息指南。

ASDM 7.7(1.150) 新增功能

发布时间：2017 年 3 月 9 日

特性	说明
管理员功能	
ASDM 升级工具的新后台服务	ASDM 采用新的 ASA/ASDM 服务执行**工具 (Tools) > 检查 ASA/ASDM 升级 (Check for ASA/ASDM Upgrades)**。未来，思科将不再使用 ASDM 早期版本所用的服务。

ASA 9.7(1)/ASDM 7.7(1) 新增功能

发布时间：2017 年 1 月 23 日

特性	说明
平台功能	

特性	说明
ASA 5506-X 系列的新默认配置，即使用集成路由和桥接	ASA 5506-X 系列将使用新的默认配置。集成桥接和路由功能提供了一种替代使用外部第 2 层交换机的方法。如果用户要更换 ASA 5505（包括硬件交换机），使用该功能可将 ASA 5505 替换为 ASA 5506-X 或其他 ASA 型号，而不必额外增加硬件。 新的默认配置包括： • GigabitEthernet 1/1 上的外部接口，从 DHCP 获取 IP 地址 • 内部桥接组 BVI 1，包含 GigabitEthernet ½ (inside1) 至 1/8 (inside7)，IP 地址 192.168.1.1 • 内部 --> 外部流量 • 内部 ---> 成员接口的内部流量 • (ASA 5506W-X) GigabitEthernet 1/9 上的 wifi 接口，IP 地址 192.168.10.1 • (ASA 5506W-X) WiFi <--> 内部，WiFi --> 外部流量 • 用于内部和 wifi 客户端的 DHCP。无线接入点本身及其所有客户端均采用 ASA 作为 DHCP 服务器。 • Management 1/1 接口启用，但未进行其他配置。然后，ASA FirePOWER 模块可使用此接口访问 ASA 内部网络并使用内部接口作为互联网网关。 • ASDM 访问 - 允许内部和 wifi 主机。 • NAT - 接口 PAT，用于从内部、wifi 和管理接口到外部的所有流量。 若要升级，您可以使用 **configure factory-default** 命令清除配置并应用默认值，也可以手动配置 BVI 和桥接组来满足需求。请注意，要使桥接组内能够轻松地进行通信，您需要启用 **same-security-traffic permit inter-interface** 命令（对于 ASA 5506W-X 默认配置，此命令已存在）。

特性	说明
ISA 3000 上支持警报端口	ISA 3000 支持两个警报输入接口和一个警报输出接口。可以将门禁感应器等外部传感器连接至警报输入。可以将蜂音器等外部设备连接到警报输出接口。触发的警报通过两个LED、系统日志、SNMP 陷阱以及连接的设备传输到警报输出接口。您可以配置外部警报说明。另外，也可以指定外部和内部警报的严重性和触发器。可以针对所有警报配置中继、监控和日志记录。 引入了以下屏幕： **配置 (Configuration) > 设备管理 (Device Management) > 警报端口 (Alarm Port) > 警报控制 (Alarm Contact)** **配置 (Configuration) > 设备管理 (Device Management) > 警报端口 (Alarm Port) > 冗余电源 (Redundant Power Supply)** **配置 (Configuration) > 设备管理 (Device Management) > 警报端口 (Alarm Port) > 温度 (Temperature)** **监控 (Monitoring) > 属性 (Properties) > 警报 (Alarm) > 警报设置 (Alarm Settings)** **监控 (Monitoring) > 属性 (Properties) > 警报 (Alarm) > 报警触点 (Alarm Contact)** **监控 (Monitoring) > 属性 (Properties) > 警报 (Alarm) > 设施警报状态 (Facility Alarm Status)**
ASAv10 上支持 Microsoft Azure 安全中心	Microsoft Azure 是一个使用专用 Microsoft Hyper V 虚拟机监控程序的公共云环境。Microsoft Azure 安全中心是基于 Azure 的 Microsoft 协调和管理层，可简化高度安全的公共云基础设施的部署。通过将 ASAv 集成到 Azure 安全中心，系统可以作为防火墙选项提供 ASAv 来保护 Azure 环境。

用于 ISA 3000 的精确时间协议 (PTP)	ISA 3000 支持 PTP - 用于网络分布式节点的时间同步协议。相比 NTP 等其他时间同步协议，该协议凭借其硬件时间戳功能可实现更高的精确性。ISA 3000支持 PTP 转发模式及一步式端到端透明时钟。我们向默认配置中添加了以下命令，以确保PTP流量不会被发送到 ASA FirePOWER 模块进行检测。如果现已拥有部署，需要手动添加这些命令：
	`object-group service bypass_sfr_inspect`
	`  service-object udp destination range 319 320`
	`access-list sfrAccessList extended deny object-group bypass_sfr_inspect any any`
	引入了以下屏幕：
	配置 (Configuration) > 设备管理 (Device Management) > PTP
	监控 (Monitoring) > 属性 (Properties) > PTP

ISA 3000 的自动备份和恢复	使用备份和恢复命令中预设的参数，您可以启用自动备份和/或自动恢复功能。这些功能的使用案例包括从外部介质执行的初始配置、设备更换、回滚至可操作状态。 引入了以下命令：**backup-package location**、**backup-package auto**、**show backup-package status**、**show backup-package summary** 无 ASDM 支持

特性	说明
防火墙功能	
支持 SCTP 多流重新排序、重组和分段。支持 SCTP 多宿主，其中 SCTP 终端拥有多个 IP 地址。	现在，系统完全支持 SCTP 多流重新排序、重组和分段，由此改善了 SCTP 流量的直径和 M3UA 检测效果。此外，系统还支持 SCTP 多宿主，其中每个终端拥有多个 IP 地址。对于多宿主，系统会对二级地址打开针孔，因此无需写入访问规则来允许这些地址。SCTP 终端必须限制为每个终端 3 个 IP 地址。 未修改任何屏幕。
M3UA 检测有所改进。	现在，M3UA 检测支持状态故障切换、半分布式集群和多宿主。另外，您还可以配置强大的应用服务器进程 (ASP) 状态验证，并验证各种消息。对于状态故障切换和集群需要使用强大的 ASP 状态验证。 修改了以下屏幕：**配置 (Configuration)** > **防火墙 (Firewall)** > **对象 (Objects)** > **检查映射 (Inspection Maps)** > **M3UA** 添加/编辑对话框。
TLS 代理和思科 Unified Communications Manager 10.5.2 版中支持 TLSv1.2。	现在，您可以对加密 SIP 的 TLS 代理使用 TLSv1.2，或对思科统一通信管理器 10.5.2 执行 SCCP 检测。TLS 代理支持作为 **client cipher-suite** 命令的一部分添加的附加 TLSv1.2 加密套件。 未修改任何屏幕。
集成路由和桥接	集成路由和桥接提供了在桥接组和路由接口之间路由的功能。桥接组指 ASA 桥接（而非路由）的接口组。ASA 并非真正的桥接，因为 ASA 仍继续充当防火墙：接口之间的访问控制受控，而且仍会执行所有常规防火墙检查。以前，您只能在透明防火墙模式下配置桥接组，而无法在桥接组之间路由。通过此功能，可以在路由防火墙模式下配置桥接组，并在桥接组之间以及桥接组与路由接口之间路由。桥接组使用桥接虚拟接口 (BVI) 作为桥接组的网关参与路由。如果 ASA 上还有额外接口可分配给桥接组，集成路由和桥接可提供替代使用外部第 2 层交换机的其他方案。在路由模式下，BVI 可以是命名接口，并可从成员接口中单独参与某些功能，例如访问规则和 DHCP 服务器。 路由模式不支持透明模式下支持的以下功能：多情景模式、ASA集群。BVI上也不支持以下功能：动态路由和组播路由。 修改了以下屏幕： **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)** > **路由 (Routing)** > **静态路由 (Static Routes)** **配置 (Configuration)** > **设备管理 (Device Management)** > **DHCP** > **DHCP 服务器 (DHCP Server)** **配置 (Configuration)** > **防火墙 (Firewall)** > **访问规则 (Access Rules)** **配置 (Configuration)** > **防火墙 (Firewall)** > **EtherType 规则 (EtherType Rules)**

特性	说明
VM 属性	在 VMware vCenter 管理的 VMware ESXi 环境下，您可以根据与一个或多个虚拟机 (VM) 相关的属性来定义过滤流量的网络对象。您可以定义访问控制列表 (ACL) 来分配用于共享一个或多个属性的 VM 组流量的策略。 添加了以下屏幕： **配置 (Configuration) > 防火墙 (Firewall) > VM 属性代理 (VM Atttribute Agent)**
用于内部网关协议的过时路由超时	现在，您可以配置超时来删除 OSPF 等内部网关协议的过时路由。 修改了以下屏幕：**配置 (Configuration) > 防火墙 (Firewall) > 高级 (Advanced) > 全局超时 (Global Timeouts)**。
路由功能	
31 位子网掩码	对于路由接口，您可在 31 位子网上配置 IP 地址来执行点对点连接。31 位子网仅包含 2 个地址；通常，该子网的第一个地址和最后一个地址预留用于网络和广播，所以不能使用 2 个地址的子网。不过，如果您拥有点对点连接，不需要网络或广播地址，则可以使用 31 位子网来保留 IPv4 地址。例如，2 个 ASA 之间的故障切换链路只需要 2 个地址；该链路一端传输的任何数据包总会被另一端接收，所以无需执行广播。另外，您还可以设立运行 SNMP 或系统日志的直连管理站。桥接组或多播路由的 BVI 不支持此功能。 修改了以下屏幕： **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)**
高可用性和扩展性功能	
FXOS 机箱上的 ASA 的站点间集群改进	现在，您可以在部署 ASA 集群时为每个 FXOS 机箱配置站点 ID。以前，您必须在 ASA 应用中配置站点 ID；此新功能简化了最初的部署。请注意，您不能再在 ASA 配置中设置站点 ID。此外，为了实现与站点间集群的最佳兼容性，我们建议您升级到 ASA 9.7(1) 和 FXOS 2.1.1，升级版包含对稳定性和性能的多项改进。 修改了以下屏幕：**配置 (Configuration) > 设备管理 (Device Management) > 高可用性和扩展性 (High Availability and Scalability) > ASA 集群 (ASA Cluster) > 集群配置 (Cluster Configuration)**
导向器本地化：改进数据中心的站点间集群	为了提高性能和保存站点内流量以便于数据中心的站点间集群，您可以启用导向器本地化。新连接通常负载均衡，并归特定站点内的集群成员所有。但是，ASA 会向任何站点的成员分配导向器角色。导向器本地化支持其他导向器角色：与所有者同一站点的本地导向器和位于任何站点的全局导向器。所有者和导向器位于同一站点有利于提高性能。另外，如果原始所有者失败，本地导向器会选择同一站点的全新连接所有者。当集群成员接收属于其他站点的连接的数据包时，使用全局导向器。 修改了以下屏幕：**配置 (Configuration) > 设备管理 (Device Management) > 高可用性和扩展性 (High Availability and Scalability) > ASA 集群 (ASA Cluster) > 集群配置 (Cluster Configuration)**

特性	说明
现在，可配置故障切换的接口链路状态监控轮询以加快检测速度	默认情况下，故障切换对中的每个 ASA 每隔 500 毫秒检查一次其接口的链路状态。现在，您可以在 300 毫秒 和 799 毫秒之间配置轮询间隔；例如，如果将轮询时间设置为 300 毫秒，ASA 则可以更快地检测接口故障并触发故障切换。 修改了以下屏幕：**配置 (Configuration)** > **设备管理 (Device Management)** > **高可用性和扩展性 (High Availability and Scalability)** > **故障切换 (Failover)** > **标准 (Criteria)**
Firepower 9300 和 4100 上支持使用双向转发检测 (BFD) 进行活动/备用故障切换运行状况监控	您可以针对 Firepower 9300 和 4100 上活动/备用对两台设备之间的故障切换运行状况检查启用双向转发检测 (BFD)。使用 BFD 执行运行状况检查比默认运行状况检查方法更可靠，而且 CPU 占用量更少。 修改了以下屏幕：**配置 (Configuration)** > **设备管理 (Device Management)** > **高可用性和扩展性 (High Availability and Scalability)** > **故障切换 (Failover)** > **设置 (Setup)**
VPN 功能	
用于 IKEv2 静态加密映射的动态 RRI	如果为**加密映射**指定**动态**，在成功建立 IPsec 安全关联 (SA) 后将发生动态反向路由注入。基于协商的选择器信息添加路由。删除 IPsec SA 后，路由也将被删除。只有基于 IKEv2 的静态加密映射中支持动态 RRI。 修改了以下屏幕：**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络(客户端)访问 (Network (Client) Access) > 高级 (Advanced) > IPsec > 加密映射 (Crypto Maps) > 添加/编辑 (Add/Edit) > 隧道策略(加密映射) (Tunnel Policy (Crypto Maps)) - 高级 (Advanced)**
ASA VPN 模块支持虚拟隧道接口 (VTI)	使用新的逻辑接口（称为“虚拟隧道接口 (VTI)”）向对等体呈现 VPN 隧道，可增强 ASA VPN 模块。这种功能支持 IPsec 配置文件连接到隧道每端的基于路由的 VPN。使用 VTI 可不必配置静态加密映射访问列表，再将它们映射至接口。 引入了以下屏幕： **配置 (Configuration)** > **站点到站点 VPN (Site-to-Site VPN)** > **高级 (Advanced)** > **IPsec 建议(转换集) (IPsec Proposals (Transform Sets))** > **IPsec 配置文件 (IPsec Profile)** **配置 (Configuration)** > **站点到站点 VPN (Site-to-Site VPN)** > **高级 (Advanced)** > **IPsec 建议(转换集) (IPsec Proposals (Transform Sets))** > **IPsec 配置文件 (IPsec Profile)** > **添加 (Add)** > **添加 Ipsec 配置文件 (Add IPsec Profile)** **配置 (Configuration)** > **设备设置 (Device Setup)** > **接口设置 (Interface Settings)** > **接口 (Interfaces)** > **添加 (Add)** > **VTI 接口 (VTI Interface)** **配置 (Configuration)** > **设备设置 (Device Setup)** > **接口设置 (Interface Settings)** > **接口 (Interfaces)** > **添加 (Add)** > **VTI 接口 (VTI Interface)** > **通用 (General)** **配置 (Configuration)** > **设备设置 (Device Setup)** > **接口设置 (Interface Settings)** > **接口 (Interfaces)** > **添加 (Add)** > **VTI 接口 (VTI Interface)** > **高级 (Advanced)**

特性	说明
适用于 AnyConnect 的基于 SAML 2.0 的 SSO	专用网络中支持基于 SAML 2.0 的运营商 IdP。使用 ASA 作为用户与服务之间的网关，利用受限的匿名 webvpn 会话来处理 IdP 上的身份验证，并转换 IdP 与用户之间的所有流量。 修改了以下屏幕：**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 无客户端 SSL VPN 访问 (Clientless SSL VPN Access) > 高级 (Advanced) > 单点登录服务器 (Single Sign On Servers) > 添加 SSO 服务器 (Add SSO Server)**。
CMPv2	为了在无线 LET 网络中担当安全网关设备，ASA 现在使用证书管理协议 (CMPv2) 支持某些管理功能。 修改了以下屏幕：**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 证书管理 (Certificate Management) > 身份证书 (Identity Certificates) > 添加身份证书 (Add an Identity Certificate)**
多个证书身份验证	现在，您可以使用 AnyConnect SSL 和 IKEv2 客户端协议验证每个会话的多个证书。为了定义多证书身份验证的协议交换并将此功能用于两种会话类型，我们对汇聚身份验证协议进行了扩展。 修改了以下屏幕： **配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络(客户端)访问 (Network (Client) Access) > 动态访问策略 (Dynamic Access Policies) > 编辑 AnyConnect 连接配置文件 (Edit AnyConnect Connection Profile)** **配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络客户端访问 (Network Client Access) > AnyConnect 连接配置文件 (AnyConnect Connection Profiles) > 编辑 AnyConnect 连接配置文件 (Edit AnyConnect Connection Profile)**
增加隧道分离 (split-tunneling) 路由限制	AC-SSL 和 AC-IKEv2 的隧道分离路由限制从 200 增至 1200。IKEv1 的限制仍保持为 200。
Chrome 上支持智能隧道	在 Mac 和 Windows 设备上，Chrome 浏览器中创建了一种支持智能隧道的新方法。Chrome 智能隧道扩展取代了 Chrome 中不再支持的 Netscape 插件应用编程接口 (NPAPI)。如果在尚未安装该扩展的 Chrome 中点击启用智能隧道的书签，系统会将您重定向到 Chrome Web Store 以获取该扩展。新安装的 Chrome 会指引用户到 Chrome Web Store 下载该扩展。该扩展会从 ASA 中下载运行智能隧道所需的二进制文件。除安装新扩展的进程之外，使用智能隧道时，常规书签和应用配置均不会改变。
无客户端 SSL VPN：所有 Web 界面的会话信息	现在，所有 Web 界面均会显示当前会话的详细信息，包括用于登录的用户名和当前分配的用户权限。这样有助于用户了解当前的用户会话及加强用户安全。
无客户端 SSL VPN：验证 Web 应用会话的所有 Cookie	现在，所有 Web 应用只有在验证与安全相关的所有 Cookie 后，才会授予访问权限。在每个请求中，系统在验证包含身份验证令牌或会话 ID 的每个 Cookie 后，才会向用户会话授予访问权限。同一请求中存在多个会话 Cookie 将导致连接断开。验证失败的 Cookie 将被视为无效，系统会向审核日志中添加事件。

特性	说明
AnyConnect：AnyConnect VPN 客户端连接的组策略现在支持最大连接时间警报间隔。	警报间隔指达到最大连接时间前的时间间隔，在该间隔后系统将向用户显示一条消息，警告他们连接断开。有效时间间隔为 1-30 分钟。默认值为 30 分钟。无客户端和站点到站点 VPN 连接以前支持该功能。 修改了以下屏幕：**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络(客户端)访问 (Network (Client) Access) > 组策略 (Group Policies) > 添加/编辑 (Add/Edit) > 通用 (General) > 更多选项 (More Options)**，添加了**最大连接时间警报间隔 (Maximum Connect Time Alert Interval)** 字段
AAA 功能	
执行 AAA 的 LDAP 和 TACACS+ 服务器支持 IPv6 地址	现在，您可以针对用于 AAA 的 LDAP 和 TACACS+ 服务器使用 IPv4 或 IPv6 地址。 修改了以下屏幕：**配置 (Configuration) > 设备管理 (Device Management) > 用户/AAA (Users/AAA) > AAA 服务器组 (AAA Server Groups) > 添加 AAA 服务器组 (Add AAA Server Group)**
管理功能	
对于所有本地 **username** 和 **enable** 密码使用 PBKDF2 散列方法	使用PBKDF2（基于密码的密钥派生功能2）散列方法，可将任何长度的本地**username** 和 **enable** 密码存储在配置中。过去，密码为 32 个字符，使用基于 MD5 的散列方法后有所缩短。现有密码将继续使用基于 MD5 的散列方法，除非您输入新的密码。如需下载指南，请参阅《常规操作配置指南》中的“软件和配置”一章。 修改了以下屏幕： **配置 (Configuration) > 设备设置 (Device Setup) > 设备名称/密码 (Device Name/Password) > 启用密码 (Enable Password)** **配置 (Configuration) > 设备管理 (Device Management) > 用户/AAA (Users/AAA) > 用户帐户 (User Accounts) > 添加/编辑用户帐户 (Add/Edit User Account) > 身份 (Identity)**
许可功能	
更改了 FXOS 机箱 上故障切换对的许可	只有活动设备才需申请许可证授权。过去，两种设备都需申请许可证授权。支持用于 FXOS 2.1.1。
监控和故障排除功能	
跟踪路由支持 IPv6 地址	为了接受 IPv6 地址，我们修改了 **traceroute** 命令。 未修改任何屏幕。
对于桥接组成员接口，支持使用 Packet Tracer	现在，对于桥接组成员接口可以使用 Packet Tracer 工具。 在 packet-tracer 屏幕中添加了 **VLAN ID** 和**目标 MAC 地址 (Destination MAC Address)** 字段：**工具 (Tools) > Packet Tracer**

特性	说明
系统日志服务器支持 IPv6 地址	现在，您可以使用 IPv6 地址来配置系统日志服务器，从而记录通过 TCP 和 UDP 的系统日志及通过它们发送系统日志。 修改了以下屏幕：**配置 (Configuration)** > **设备管理 (Device Management)** > **日志记录 (Logging)** > **系统日志服务器 (Syslog Servers)** > **添加系统日志服务器 (Add Syslog Server)**
SNMP OID 和 MIB	现在，ASA 支持与端到端透明时钟模式（属于 ISA 3000 精确时间协议 (PTP) 的一部分）相应的 SNMP MIB 对象。支持以下 SNMP MIB 对象： • ciscoPtpMIBSystemInfo • cPtpClockDefaultDSTable • cPtpClockTransDefaultDSTable • cPtpClockPortTransDSTable

升级软件

本节提供完成升级的升级路径信息和链接。

升级路径

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。

当前 **ASA** 版本	首先升级到：	然后升级到：
8.2(x) 及更早版本	8.4(5)	9.1(3) 及更高版本
8.3(x)	8.4(5)	9.1(3) 及更高版本
8.4(1) 至 8.4(4)	8.4(5) 或 9.0(2+)	9.1(3) 及更高版本
8.4(5+)	—	9.1(3) 及更高版本
8.5(1)	9.0(2+)	9.1(3) 及更高版本
8.6(1)	9.0(2+)	9.1(3) 及更高版本
9.0(1)	9.0(2+)	9.1(3) 及更高版本
9.0(2+)	—	9.1(3) 及更高版本
9.1(1)	9.1(2)	9.1(3) 及更高版本

当前 ASA 版本	首先升级到：	然后升级到：
9.1(2+)	—	9.1(3) 及更高版本
9.2(x)	-	9.2(2) 及更高版本
9.3(x)	-	9.3(2) 及更高版本
9.4(x)	-	9.4(2) 及更高版本
9.5(x)	—	9.5(2) 及更高版本
9.6(x)	—	9.6(2) 及更高版本
9.7(x)	—	9.8(1) 及更高版本

升级链接

要完成升级，请参阅升级到 ASA 9.7 和 ASDM 7.7。

遗留和已修复的漏洞

可通过思科缺陷搜索工具查看这一版本中尚未解决和已解决的缺陷。通过这一基于 Web 的工具，您可以访问思科缺陷追踪系统，其中记录了关于此本产品和其他思科硬件及软件产品的缺陷和漏洞信息。

注释 您必须拥有 Cisco.com 帐户才能登录并访问思科缺陷搜索工具。如果没有，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。

有关思科漏洞搜索工具的详细信息，请参阅 漏洞搜索工具帮助及常见问题。

遗留漏洞

本节列出了每个版本的遗留漏洞。

版本 7.7(1.150) 中的遗留漏洞

版本 7.7(1.150) 中没有新的遗留漏洞。请参阅版本 7.7(1) 中的遗留漏洞 ， 第 20 页。

版本 7.7(1) 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 7.7(1) 版本中严重程度在 3 级及以上的所有漏洞：

- 7.7(1) 遗留漏洞搜索。

下表列出了在发布此版本说明时存在的遗留漏洞。

警告 ID 编号	说明
CSCvc73791	asdm 配置中的 SNMPv3 用户出现故障。

已修复的漏洞

本节列出了每个版本的已修复漏洞。

版本 7.7(1.150) 中的已修复漏洞

我们尚未解决此版本中的任何漏洞。

版本 7.7(1) 中的已修复漏洞

如果您拥有思科支持合同，请按照以下程序搜索严重性为 3 级及更高级别的已修复漏洞：

- 7.7(1) 已修复漏洞搜索。

下表列出了本版本说明发布时已修复的漏洞。

警告 ID 编号	说明
CSCva50676	ASDM 使用访问列表中基于主机的对象替换网络 IP
CSCva89785	ASDM：服务策略下的 TCP 超时值向 ASA 推送错误值
CSCva91507	ASDM 不支持 0 至 65535 范围的端口
CSCva99049	ASDM：重新排序列表后添加的服务对象错误
CSCvb16663	ASDM 7.6.2 无法显示 VPN 会话 - 卡在 97% 加载位置
CSCvb24760	ASDM：从启动程序和 cisco.com 中取消演示功能
CSCvb37828	ASDM 7.6.x 不显示“pre-fill-username”选项
CSCvb48973	ASDM：VPN 向导的配置组合不正确

警告 ID 编号	说明
CSCvb49232	ASDM：VPN 删除加密访问列表
CSCvb53989	ASDM 禁止更正非连续对象子网掩码
CSCvb63008	ASDM 7.6.2 不显示活跃的 Anyconnect 客户端
CSCvb68442	ASDM 文件管理不显示 Disk1
CSCvb99770	ASDM 不删除 ACL 中不同行号的相同注释
CSCvb99824	从 ACE 中删除对象组时，ASDM 添加的注释重复
CSCvc10201	ASDM 7.6.2 无法显示 IPsec RA VPN 会话 - 卡在 97% 加载位置

最终用户许可协议

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

相关文档

有关 ASA 的更多信息，请参阅导航思科 ASA 系列文档。