Secure Firewall ASA 简介

Cisco Secure Firewall ASA 在一台设备。ASA 包括许多高级功能，例如多安全情景（类似于虚拟化防火墙）、集群（将多个防火墙组合成一个防火墙）、透明（第 2 层）防火墙或路由（第 3 层）防火墙操作、高级检测引擎、IPsec VPN、SSL VPN 和无客户端 SSL VPN 支持以及许多其他功能。

注释 ASDM 支持许多 ASA 版本。ASDM 文档和在线帮助包括 ASA 支持的所有最新功能。如果您运行的是旧版ASA软件，本文档可能包含您的版本中不支持的功能。请参阅每章的功能历史记录表以确定功能的添加时间。有关每个 ASA 版本所支持的 ASDM 最低版本，请参阅思科 ASA 兼容性。另请参阅特殊服务、弃用的服务和传统服务，第 13 页。

ASDM 要求

ASDM Java 要求

您可以使用 Oracle JRE 8.0 (**asdm-*version*.bin**) 或 OpenJRE 1.8.x (**asdm-openjre-*version*.bin**) 安装 ASDM。

注释 ASDM 未在 Linux 上测试。

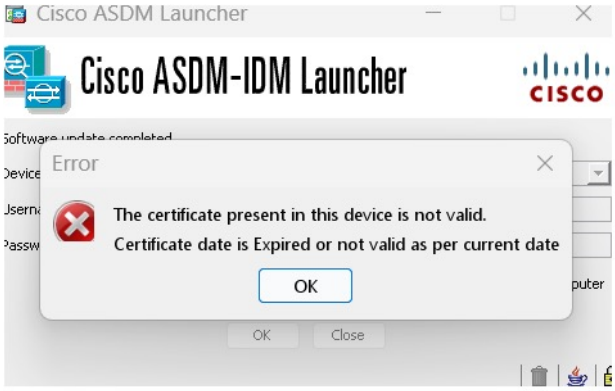
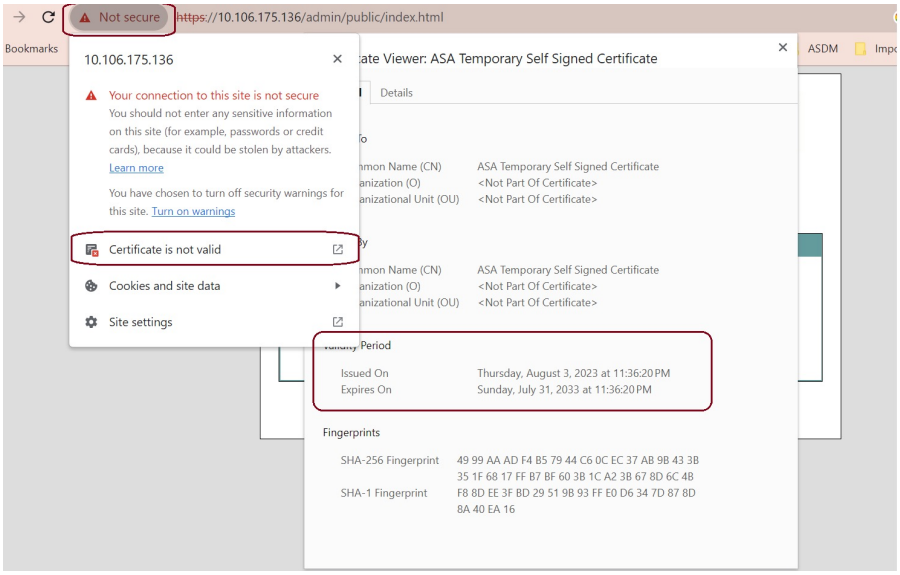
表 *1: ASDM* 操作系统和浏览器要求

操作系统	浏览器			Oracle JRE	OpenJRE
	Firefox	Safari	Chrome		
Microsoft Windows（英文版和日文版）： • 11 • 10 注释 如果您遇到 ASDM 快捷方式问题，请参阅 ASDM 兼容性说明，第 2 页 中的 Windows 10。 • 8 • 7 • Server 2016 和 Server 2019 • Server 2012 R2 • Server 2012 • Server 2008	是	不支持	是	8.0 版本 8u261 或更高版本	1.8 注释 不支持 Windows 7 或 32 位
Apple OS X 10.4 及更高版本	兼容	兼容	是（仅限 64 位版本）	8.0 版本 8u261 或更高版本	1.8

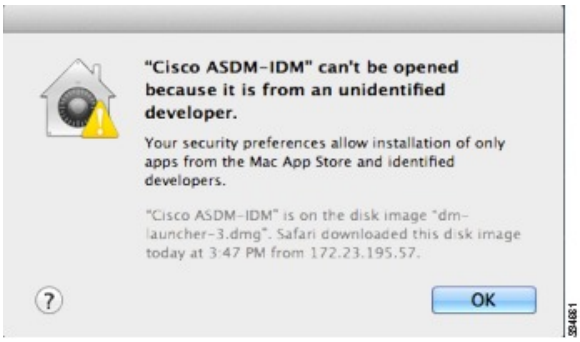
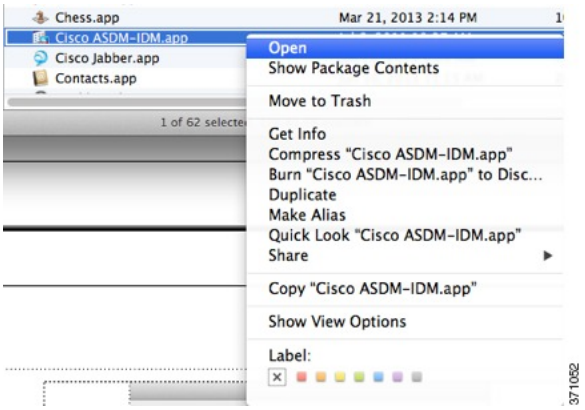
ASDM 兼容性说明

下表列出了 ASDM 兼容性警告。

条件	说明
ASDM 启动器与 ASDM 版本的兼容性	“无法启动设备管理器” 错误消息。 如果升级到新的 ASDM 版本后出现此错误，则可能需要重新安装最新的启动程序。 **1.** 在 ASA 上打开 ASDM 网页：https://<asa_ip_address> 。 **2.** 点击 **安装 ASDM 启动程序**。 图 *1:* 安装 ***ASDM*** 启动程序  **3.** 将用户名和密码字段留空（适用于新安装），然后点击**确定 (OK)**。 如果未配置 HTTPS 身份验证，可以在没有用户名和 **enable** 密码（默认为空）的情况下获得对 ASDM 的访问权限。首次在 CLI 中输入 **enable** 命令时，系统会提示您更改密码；登录 ASDM 时不会强制执行此行为。建议您尽快更改启用密码，不要再保持空白状态。。**注意**：如果您启用了 HTTPS 身份验证，则输入您的用户名及关联的密码。即使不使用身份验证，如果您在登录屏幕输入用户名和密码（而不是将用户名留空），ASDM 也会从本地数据库中检查是否有匹配项。

条件	说明
由于时间和日期与 ASA 不匹配，自签名证书无效	ASDM 会验证自签名 SSL 证书，如果 ASA 的日期不在证书的**颁发日期**和**到期日期**内，则 ASDM 不会启动。如果时间和日期不匹配，您将看到以下错误： **图 *2:* 证书无效**  **要解决此问题，请执行以下操作：**在 ASA 上设置正确的时间并重新加载。 要检查证书日期（显示的示例为 Chrome），请执行以下操作： **1.** 转至 https://*device_ip*。 **2.** 点击菜单栏中的**不安全 (Not secure)** 文本。 **3.** 点击**证书无效 (Certificate is not valid)** 以打开“证书查看器”。 **4.** 检查有效期。 **图 *3:* 证书查看器** 

条件	说明
Windows Active Directory 目录访问权限	在某些情况下，Windows 用户的 Active Directory 设置可能会限制对在 Windows 上成功启动 ASDM 所需的程序文件位置进行访问。需要对以下目录的访问权限： • “桌面”文件夹 • C:\Windows\System32C:\Users\<username>\.asdm • C:\Program Files (x86)\Cisco Systems 如果 Active Directory 限制了目录访问，则需要向 Active Directory 管理员请求访问权限。
Windows 10	**“此应用无法在您的 PC 上运行”**错误消息。 当您安装 ASDM 启动程序时，Windows 10 可能会将 ASDM 快捷方式目标替换为 Windows 脚本主机路径，这会导致此错误。要修复快捷方式目标，请执行以下操作： **1.** 依次选择**启动 (Start)** > **思科 ASDM-IDM 启动程序 (Cisco ASDM-IDM Launcher)**，然后右键点击**思科 ASDM-IDM 启动程序 (Cisco ASDM-IDM Launcher)** 应用。 **2.** 选择**更多** > **打开文件位置**。 Windows 将打开带有快捷方式图标的目录。 **3.** 右键点击快捷方式图标，然后选择**属性 (Properties)**。 **4.** 将**目标**更改为： **C:\Windows\System32\wscript.exe invisible.vbs run.bat** **5.** 点击**确定 (OK)**。
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。

条件	说明
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. 要使 ASDM 运行，请右击（或者按住 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窗口；但您可以通过该窗口打开ASDM。点击**打开 (Open)**。系统将打开 ASDM-IDM Launcher。 

条件	说明
ASA 需要有强加密许可证 (3DES/AES) 注释 智能许可模式允许在没有强加密许可证的情况下使用 ASDM 进行初始访问。	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. 转到 www.cisco.com/go/license。 2. 点击**继续产品许可证注册 (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**产品 (Product)** 列表中选择**思科 ASA 3DES/AES 许可证 (Cisco ASA 3DES/AES License)**，然后点击**下一步 (Next)**。 7. 输入 ASA 的序列号，然后按照提示为 ASA 申请 3DES/AES 许可证。
• 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）。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。我们建议重新启用其中一种算法（请参阅**配置 (Configuration)** > **设备管理 (Device Management)** > **高级 (Advanced)** > **SSL 设置 (SSL Settings)** 窗格）；或者可以在 Chrome 中使用 **--disable-ssl-false-start** 标记根据使用标记运行 Chromium 来禁用 SSL 虚假启动。

硬件和软件兼容性

有关受支持硬件和软件的完整列表，请参阅《思科 ASA 兼容性》。

VPN 兼容性

请参阅受支持的 VPN 平台（思科 ASA 系列）。

新增功能

本部分列出了每个版本的新功能。

注释 系统日志消息指南中列出了新增的、更改的和已弃用的系统日志消息。

ASA 9.22(1)/ASDM 7.22(1)的新功能

发布日期：**2023** 年 **7** 月

特性	说明
平台功能	
防火墙功能	
高可用性和扩展性功能	
Cisco Secure Firewall 3100 和 4200 个最大集群节点增加到 16 个。	对于 Cisco Secure Firewall 3100 和 4200，最大节点数从 8 增加到 16。
Cisco Secure Firewall 3100 和 4200 集群独立接口模式	独立接口是正常的路由接口，每个接口都有自己的 本地 *IP* 地址 用于路由。每个接口的 主集群 *IP* 地址 是固定地址，始终属于控制节点。当控制节点更改时，主集群 IP 地址将转移到新的控制节点，使集群的管理得以无缝继续。 必须在上游交换机上分别配置负载均衡。 新增/修改的命令：**cluster interface-mode individual** 新增/修改的命令：向导 > > 高可用性和可扩展性向导
路由功能	
接口功能	
许可证功能	
证书功能	
管理、监控和故障排除功能	
VPN 功能	
ASDM 功能	

防火墙功能概述

防火墙可防止外部网络上的用户在未经授权的情况下访问内部网络。防火墙同时可以为不同的内部网络提供保护，例如将人力资源网络与用户网络分开。如果需要向外部用户提供某些网络资源（例如 Web 服务器或 FTP 服务器），可以将这些资源放置在防火墙后面单独的网络上（这种网络称为隔离区 (DMZ)）。防火墙允许有限访问 DMZ，但由于 DMZ 只包括公共服务器，因此发生在这个位置的攻击只会影响到服务器，而不会影响其他内部网络。还可以通过以下手段来控制内部用户何时可以访问外部网络（例如，访问互联网）：仅允许访问某些地址，要求身份验证或授权，配合使用外部 URL 过滤服务器。

讨论连接到防火墙的网络时，外部网络位于防火墙之前，内部网络可以得到保护，位于防火墙之后，*DMZ* 虽然位于防火墙之后，却可以限制外部用户的访问权限。由于 ASA 允许您配置许多安全策略不同的接口，包括许多内部接口、许多 DMZ 甚至许多外部接口（如果需要），则仅按照常规含义使用这些术语。

安全策略概述

安全策略确定哪些流量可通过防火墙来访问其他网络。默认情况下，ASA 允许流量从内部网络（较高安全性级别）自由流向外部网络（较低安全性级别）。可以将操作应用于流量，以自定义安全策略。

通过访问规则允许或拒绝流量

您可以应用访问规则，以限制从内部到外部的流量，或者允许从外部到内部的流量。对于网桥组接口，还可以应用 EtherType 访问规则来允许非 IP 流量。

应用 NAT

NAT 的一些优势如下：

- 可以在内部网络上使用专用地址。专用地址不能在互联网上进行路由。
- NAT 可隐藏其他网络的本地地址，使攻击者无法获悉主机的真实地址。
- NAT 可通过支持重叠 IP 地址来解决 IP 路由问题。

保护 IP 片段

ASA 提供 IP 片段保护。此功能对所有 ICMP 错误消息执行完全重组，并对通过 ASA 路由的剩余 IP 片段执行虚拟重组。系统会丢弃并记录未能通过安全检查的片段。不能禁用虚拟重组。

应用 HTTP、HTTPS 或 FTP 过滤

虽然可以使用访问列表来防止对于特定网站或 FTP 服务器的出站访问，但由于互联网的规模和动态性质，以这种方式配置和管理网络使用并不切合实际。

可以在 ASA 上配置云网络安全。您还可以将 ASA 与思科网络安全设备 (WSA) 等外部产品结合使用。

应用应用检测

针对在用户数据包内嵌入 IP 寻址信息的服务或在动态分配端口上打开辅助信道的服务，需要使用检测引擎。这些协议要求 ASA 执行深度数据包检测。

应用 QoS 策略

某些网络流量（例如声音和流传输视频）不允许出现长时间延迟。QoS 是一种网络功能，使您可以向此类流量赋予优先级。QoS 是指一种可以向所选网络流量提供更好服务的网络功能。

应用连接限制和 TCP 规范化

可以限制TCP连接、UDP连接和半开连接。限制连接和半开连接的数量可防止遭受DoS攻击。ASA 通过限制初期连接的数量来触发 TCP 拦截，从而防止内部系统受到 DoS 攻击（这种攻击使用 TCP SYN 数据包对接口发起泛洪攻击）。半开连接是源与目标之间尚未完成必要握手的连接请求。

TCP 规范化是指一种包含高级 TCP 连接设置的功能，用以丢弃有异常迹象的数据包。

启用威胁检测

可以配置扫描威胁检测和基本威胁检测，还可以配置如何使用统计信息来分析威胁。

基本威胁检测会检测可能与攻击（例如 DoS 攻击）相关的活动，并自动发送系统日志消息。

典型的扫描攻击包含测试子网中每个IP地址可达性（通过扫描子网中的多台主机或扫描主机或子网中的多个端口）的主机。扫描威胁检测功能确定主机何时执行扫描。ASA 扫描威胁检测功能与基于流量签名的 IPS 扫描检测不同，前者维护着一个广泛的数据库，其中包含可用来分析扫描活动的主机统计信息。

主机数据库跟踪可疑的活动（例如没有返回活动的连接、访问关闭的服务端口、如非随机IPID等易受攻击的 TCP 行为以及更多行为）。

您可以将 ASA 配置为发送有关攻击者的系统日志消息，也可以自动避开主机。

防火墙模式概览

ASA 在两种不同的防火墙模式下运行：

- 路由
- 透明

在路由模式下，ASA 被视为网络中的一个路由器跃点。

在透明模式下，ASA 如同是“线缆中的块”或“隐蔽的防火墙”，不被视为路由器跃点。ASA 在“网桥组”中连接至其内部和外部接口上的同一子网。

您可以使用透明防火墙简化网络配置。如果希望防火墙对攻击者不可见，透明模式同样有用。还可以针对在路由模式中会以其他方式被阻止的流量使用透明防火墙。例如，透明防火墙可通过EtherType访问列表允许组播数据流。

路由模式支持集成路由和桥接，因此也可以在路由模式下配置网桥组，并在网桥组和普通接口之间路由。在路由模式下，您可以复制透明模式功能；如果您不需要多情景模式或集群，可以考虑改用路由模式。

状态监测概览

系统使用自适应安全算法检测通过ASA的所有流量，要么允许通过，要么将其丢弃。简单的数据包过滤器可以检查源地址、目标地址和端口是否正确，但不会检查数据包序列或标记是否正确。过滤器还可以根据过滤器本身检查每个数据包，但这个过程可能比较慢。

注释 TCP 状态绕行功能使您可以自定义数据包流量。

但 ASA 等状态防火墙会考虑数据包的状态：

- 这是新连接吗？

  如果是新连接，ASA 必须对照访问列表检查数据包，并执行其他任务以确定允许还是拒绝数据包。为了执行此检查，会话的第一个数据包将通过“会话管理路径”，根据流量类型，它还可能通过“控制平面路径”。

  会话管理路径负责执行以下任务：

  - 执行访问列表检查
  - 执行路由查找
  - 分配 NAT 转换 (xlate)
  - 在“快速路径”中建立会话

  ASA 会在快速路径中为 TCP 流量创建转发和反向流；ASA 还会为无连接协议（例如 UDP、ICMP）创建连接状态信息（启用 ICMP 检测时），以便它们也可以使用快速路径。

注释 对于其他IP协议，例如SCTP，ASA不会创建反向流路径。因此，涉及这些连接的 ICMP 错误数据包将被丢弃。

  需要第 7 层检测的某些数据包（必须检测或改变数据包负载）会传递到控制平面路径。具有两个或多个信道（一个使用已知端口号的数据信道，一个对每个会话使用不同端口号的控制信道，）的协议需要第 7 层检测引擎。这些协议包括 FTP、H.323 和 SNMP。

- 这是已建立的连接吗？

如果连接已建立，则ASA不需要重新检查数据包；多数匹配的数据包都可以双向通过“快速”路径。快速路径负责执行以下任务：

- IP 校验和验证
- 会话查找
- TCP 序列号检查
- 基于现有会话的 NAT 转换
- 第 3 层和第 4 层报头调整

需要第 7 层检测的协议的数据包也可以通过快速路径。

某些建立的会话数据包必须继续通过会话管理路径或控制平面路径。通过会话管理路径的数据包包括需要检测或内容过滤的 HTTP 数据包。通过控制平面路径的数据包包括需要第 7 层检测的协议的控制数据包。

VPN 功能概述

VPN 是一个跨 TCP/IP 网络（例如互联网）的安全连接，显示为私有连接。这种安全连接被称为隧道。ASA 使用隧道传输协议协商安全参数，创建和管理隧道，封装数据包，通过隧道收发数据包，然后再对它们解除封装。ASA 相当于一个双向隧道终端：可以接收普通数据包，封装它们，再将它们发送到隧道的另一端，在那里系统将对数据包解除封装并将其发送到最终目标。它也可以接收已封装的数据包，解除数据包封装，然后将它们发送到最终目标。ASA 可调用各种标准协议来完成这些功能。

ASA 可执行以下功能：

- 建立隧道
- 协商隧道参数
- 对用户进行身份验证
- 分配用户地址
- 数据加密和解密
- 管理安全密钥
- 管理隧道范围内的数据传输
- 按隧道终端或路由器方式管理入站和出站数据传输

ASA 可调用各种标准协议来完成这些功能。

安全情景概述

您可以将一台 ASA 设备分区成多个虚拟设备，这些虚拟设备被称为安全情景。每个 context 都是一台独立设备，拥有自己的安全策略、接口和管理员。多情景类似于拥有多台独立设备。多情景模式支持很多功能，包括路由表、防火墙功能、IPS 和管理；但是，某些功能不受支持。有关详细信息，请参阅相关功能章节。

在多情景模式中，ASA 包括用于每个情景的配置，其中确定安全策略、接口以及可以在独立设备中配置的几乎所有选项。系统管理员可在系统配置中配置情景以添加和管理情景；系统配置类似于单模式配置，是启动配置。系统配置可标识ASA的基本设置。系统配置本身并不包含任何网络接口或网络设置；相反，当系统需要访问网络资源（例如，从服务器下载情景）时，它使用指定为管理情景的某个情景。

管理情景类似于任何其他情景，唯一不同之处在于，当用户登录管理情景时，该用户拥有系统管理员权限并能访问系统和所有其他情景。

ASA 集群概述

通过ASA集群，您可以将多台ASA组合成单个逻辑设备。集群具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。

只能在控制设备上执行所有配置（引导程序配置除外）；然后配置将被复制到成员设备中。

特殊服务、弃用的服务和传统服务

对于某些服务，可以在主配置指南和在线帮助以外找到相关文档。

特殊服务指南

特殊服务使 ASA 可以与其他思科产品实现互操作；例如，为电话服务提供安全代理（统一通信），同时提供僵尸网络流量过滤和思科更新服务器上的动态数据库，或者为思科网络安全设备提供 WCCP 服务。某些特殊服务在单独的指南中进行介绍：

- 思科 ASA 僵尸网络流量过滤器指南
- 思科 ASA NetFlow 实施指南
- 思科 ASA 统一通信指南
- 思科 ASA WCCP 流量重定向指南
- SNMP 版本 3 工具实施指南

弃用的服务

有关弃用的功能，请参阅相应ASA版本的配置指南。同样，对于重新设计的功能（例如，版本 8.2 与版本 8.3 之间 NAT，或版本 8.3 与版本 8.4 版之间的透明模式接口），请参阅相应版本的

配置指南。虽然 ASDM 向后兼容之前的 ASA 版本，但配置指南和在线帮助仅涵盖有关最新版本的内容。

传统服务指南

ASA 仍支持传统服务，但可能还有更好的替代服务可供使用。传统服务在单独的指南中进行介绍：

思科 ASA 传统功能指南

本指南包含以下章节：

- 配置 RIP
- 适用于网络接入的 AAA 规则
- 使用保护工具，其中包括防止 IP 欺骗 (**ip verify reverse-path**)、配置分段大小 (**fragment**)、阻止不需要的连接 (**shun**)、配置 TCP 选项（适用于 ASDM）以及为基本 IPS 支持配置 IP 审核 (**ip audit**)。
- 配置过滤服务

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。