



## 简介

本文档中的信息可帮助您在 4100 和 9300 平台设备上强化思科 Firepower 可扩展操作系统 (FXOS)，从而提高网络的整体安全性。有关 Firepower 部署的其他组件的强化信息，请参阅以下文档：

- [《思科 ASA 防火墙强化指南》](#)
- [《思科 Firepower 管理中心强化指南，版本 6.4》](#)
- [《思科 Firepower 威胁防御强化指南，版本 6.4》](#)

网络包含三个功能性平面 — 管理、控制和数据，每个平面具备不同的功能，必须得到保护。

### 管理平面

管理平面包含支持思科 FXOS 配置、维护和监控功能的所有流量的逻辑组。此组中的流量包括 HTTP/HTTPS、SSH、FTP、简单网络管理协议 (SNMP)、系统日志、TACACS+、远程验证拨入用户服务 (RADIUS) 和 DNS。管理平面流量始终定向到本地的思科 FXOS。

### 控制平面

控制平面包含用于创建和维护网络和接口（例如链路层发现协议 (LLDP) 和链路聚合控制协议 (LACP)）状态的所有交换、信令、链路状态及其他控制协议的逻辑组。控制平面流量始终定向到本地的思科 FXOS 设备。

### 数据平面

数据平面包含由主机、客户端、服务器和应用程序生成的客户应用程序流量的逻辑组，这些流量源自并流向网络支持的其他类似设备。

本文档分为三个部分：

- 保护网络运营
- 管理平面强化
- 用户管理

虽然本文档大部分内容用于说明保护思科 FXOS 设备配置的安全，但是仅通过配置不能完全保护网络的安全。就对安全性的意义而言，网络上所用的操作程序及网络管理人员与基础设施设备的配置同等重要。本文档酌情提供有助于保护思科 FXOS 部署的实施建议。

- [安全认证合规性，第 2 页](#)

# 安全认证合规性

请注意，您的组织只能使用符合由美国国防部和其他政府认证机构制定的安全标准的设备和软件。

根据证书特定的指导文档进行配置时，Firepower 系统可确保符合以下认证标准：

- 通用标准 (CC)：国际共同标准承认协定建立的全球标准，用于定义对安全产品的要求。
- 国防部信息网络获批产品列表 (DoDIN APL)：符合美国国防信息系统机构 (DISA) 建立的安全要求的产品列表。注意：美国政府已将统一功能获批产品列表 (UCAPL) 的名称改为 DODIN APL。Firepower 文档和 Firepower 管理中心 Web 界面中对 UCAPL 的引用可以解释为对 DoDIN APL 的引用。
- 联邦信息处理标准 (FIPS) 140：针对加密模块的要求规范。

认证指导文档在产品认证完成后将单独提供；本强化指南的发布并不保证完成任何产品认证。

## 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。