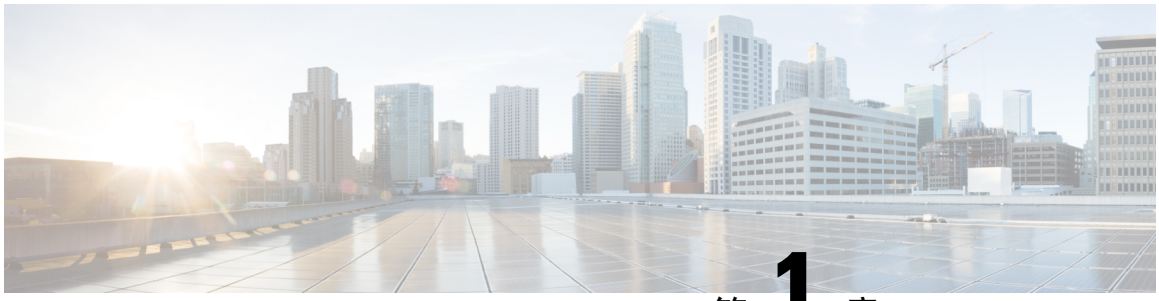
《思科 Firepower 4100/9300 强化指南》

首次发布日期: 2019 年 5 月 10 日

上次修改日期: 2023 年 6 月 22 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



第 1 章

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

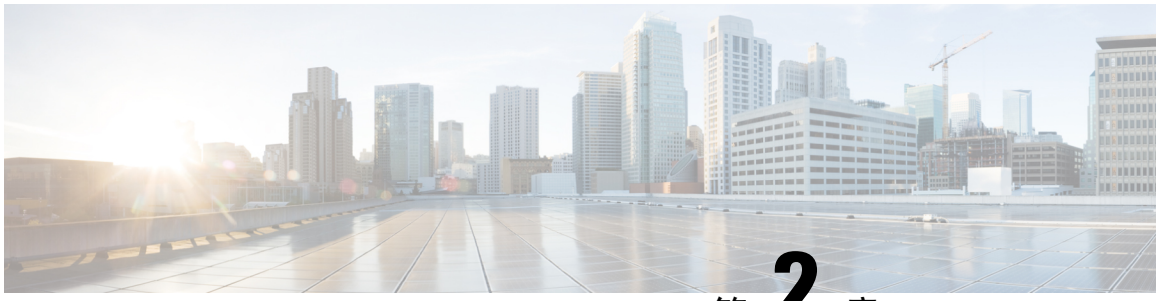
安全认证合规性

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。



第 2 章

保护网络运营

保护网络运营是一个非常重要的话题。虽然本文档大部分内容用于说明保护运行 FXOS 的 Firepower 4100/9300 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。

以下章节包含 FXOS 管理员推荐实施的操作建议。以下章节重点说明了网络操作的特定关键区域，但不是很全面。

监控思科安全公告

思科产品安全事件响应团队 (PSIRT) 针对与思科产品相关的安全问题创建和维护出版物（通常称为“思科安全建议”）。可至以下网址查看安全建议：http://www.cisco.com/go/psirt。

有关思科 PSIRT 漏洞报告的信息，请参阅《思科安全漏洞策略》。

为维护系统安全，思科 FXOS 管理员应了解思科安全建议中传达的信息。在评估漏洞可能对网络造成的威胁之前，需要详细了解漏洞。如需与此评估流程相关的帮助，请参阅安全漏洞公告风险分类。

更新到 FXOS 的最新版本

FXOS 的每个新平台套件版本中都包含重要的安全更新。我们建议您尽快将 FXOS 系统更新至最新的可用版本。

有关各种配置中 FXOS 支持的兼容性和升级路径的更多信息，请参阅 Cisco.com 上的《思科 *FIREPOWER 4100/9300 FXOS* 兼容性指南》和《思科 *Firepower 4100/9300* 升级指南》。

自定义登录前横幅

您可以指定用户在登录 Firepower 机箱管理器或 FXOS CLI 之前，FXOS 向用户显示的消息。从强化的角度来说，应使用此消息来阻止未经授权的访问。

以下 CLI 示例为 FXOS 机箱管理器和 FXOS CLI 创建登录前横幅：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # create pre-login-banner
Firepower-chassis /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED
 You must have explicit, authorized permission to access or configure this device.
 Unauthorized attempts and actions to access or use this system may result in civil and/or

criminal penalties.
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```

启用通用标准或 FIPS 模式

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，您可以启用通用标准或FIPS模式，通过单个设置应用多个强化更改。请注意，如果您的组织不必遵守安全认证合规标准，您仍然可以为FXOS启用FIPS或通用标准模式，但请注意，这可能会导致设备上出现兼容性问题。

启用通用标准或 FIPS 模式的选项显示在 Firepower 机箱管理器 Web 界面的**平台设置 (Platform Settings)** > **FIPS/通用标准 (FIPS/Common Criteria)**模式下。

注释

- 启用安全认证合规性不保证严格符合所选安全模式的所有要求。本文档介绍了一些额外设置，这些设置可以增强您的部署，使之比通用标准或FIPS模式提供的部署更加强大。有关确保完全合规所需的强化程序的完整信息，请参阅由认证实体提供的此产品的相关规定。
- 在启用 FIPS、通用标准或两者时，使用 FIPS 兼容工具进行设备访问。

保护网络时间协议 (NTP)

我们强烈建议使用信任的网络时间协议 (NTP) 服务器同步 Firepower 4100/9300 FXOS 设备及其关联服务器上的系统时间。

要为 FXOS 启用 NTP，必须先生成 NTP 密钥 ID 和密钥值，然后在 FXOS 机箱管理器中按照以下工作流程将 NTP 服务器添加到 FXOS 机箱：**Platform Settings > Set Time Source > Use NTP Server**。要进一步强化 NTP，请配置 NTP 服务器身份验证。

有关如何为 FXOS 配置 NTP 服务器和 NTP 服务器身份验证的完整说明，请参阅《思科 *Firepower 4100/9300 FXOS CLI* 配置指南》“平台设置”一章的使用 NTP 设置日期和时间主题。

注释

- 启用后，NTP 身份验证功能全局适用于与 FXOS 关联的所有已配置服务器。
- 仅支持使用 SHA1 进行 NTP 服务器身份验证。
- 您需要密钥 ID 和密钥值，才能进行服务器身份验证。密钥 ID 用于告知客户端和服务器在计算消息摘要时要使用哪个密钥值。密钥值是使用 nip-keygen 得出的固定值。

保护域名系统 (DNS)

网络环境中相互通信的计算机依赖于 DNS 协议来提供 IP 地址和主机名之间的映射。

DNS 可能容易受到特定类型的攻击，这些攻击会利用 DNS 服务器中未配置安全防护措施的薄弱点。确保您的本地 DNS 服务器配置符合行业建议的安全最佳实践；思科在此文档中提供了指导原则：https://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html。

利用身份验证、授权和记帐

身份认证、授权和记帐 (AAA) 框架对于保护对网络设备的交互式访问至关重要。AAA 框架提供可根据网络需求量身定制的高度可配置环境。

FXOS 系统支持 RADIUS 和 TACACS+。TACACS+ 会将整个 TCP 负载加密，包括用户名和密码。Radius 只会将密码加密。此外，TACACS+ 还提供命令授权，而 RADIUS 仅提供身份验证和计帐。因此，我们建议您使用 TACACS + 实现最高的身份验证安全性。

此外，您还可以使用 LDAP 进行用户验证。要对 LDAP 身份验证交换加密，请采用 CLI 选项以使用 SSL。

```
Firepower /security/ldap/server # set ssl yes
```

有关如何配置 AAA 的详细信息和完整程序，请参阅《思科 *FIREPOWER 4100/9300 FXOS CLI* 配置指南》中“平台设置”一章的“配置 AAA”部分。

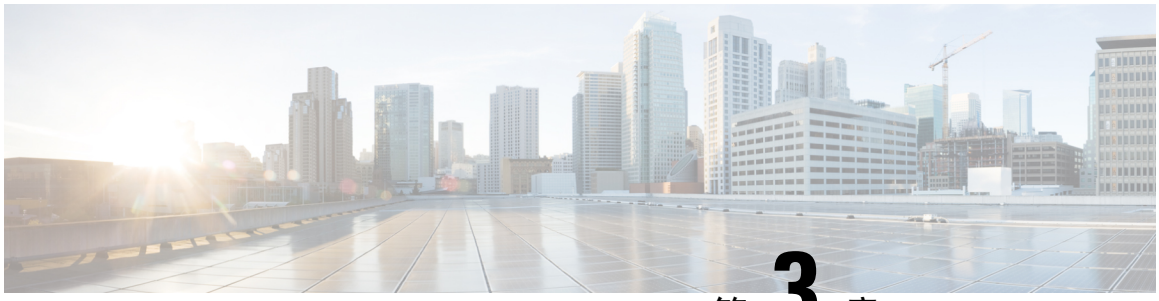
使用安全协议

思科 FXOS 利用多种协议来传送敏感的网络管理数据。您必须尽可能地使用安全协议。安全协议选择包括使用 SSH 而不是 Telnet，以便将认证数据和管理信息都加密。此外，在复制配置数据时，您必须使用安全文件传输协议。例如，使用安全复制协议 (SCP) 代替 FTP 或 TFTP。有关如何使用安全协议的其他详细信息，请参阅本文档的管理平面，第 7 页部分。

配置管理

配置管理是对配置更改提出建议、审核、批准和部署的过程。

思科 FXOS 设备的配置包含许多敏感的详细信息，包括用户名、密码和访问控制列表 (ACL) 的内容。用于存档思科 FXOS 设备配置的存储库应该是安全的，并且访问应该仅限于那些需要访问的角色和功能。对于这些信息的不安全访问可能破坏整个网络的安全。



第 3 章

管理平面

管理平面包含用于实现网络管理目标的功能。这些目标包括使用 SSH 的交互式管理会话，以及使用 SNMP 收集的统计信息。考虑网络设备的安全时，确保管理平面受到保护至关重要。如果安全事件影响到管理平面的功能，则可能无法恢复网络或使其保持稳定。

以下部分详细说明思科 FXOS 中有助于强化管理平面的安全特性和配置：

强化管理平面

管理平面用于访问、配置和管理设备，以及监控设备的操作及其所处的网络。管理平面接收并发送流量以支持这些功能运行。必须要保护设备管理平面和控制平面的安全，因为控制平面的运行直接影响管理平面的运行。以下列表包含管理平面使用的协议：

- SNMP
- Telnet
- SSH
- SFTP
- FTP

- TFTP
- HTTP/HTTPS
- 安全复制协议 (SCP)
- TACACS+
- RADIUS
- LDAP
- 网络时间协议 (NTP)
- Syslog

发生安全事件时，管理员必须采取相应措施确保管理平面和控制平面的完好性。如果其中一个平面被成功利用，则所有平面都可能遭到破坏。

控制和加密管理会话

因为信息可能会在交互式管理会话期间泄露，所以必须加密此流量，确保恶意用户无法读取正在传输的数据。加密流量允许对设备进行安全远程访问连接。如果通过网络以纯文本形式发送管理会话的流量，攻击者可以获取有关设备和网络的敏感信息。FXOS 上支持以下协议：

- SSH
- TLS
- HTTPS
- SNMP
- LDAP
- Telnet

注释 Telnet 不是安全协议，我们建议 FXOS 管理员不要使用它。

以下部分将详细介绍管理会话协议的强化配置选项。

安装受信任身份证书

在完成初始配置后，系统将生成自签名 SSL 证书，以便与 FXOS 机箱 Web 应用程序一起使用。由于该证书是自签名证书，客户端浏览器不会自动信任它。新的客户端浏览器首次访问 FXOS 机箱 Web 界面时，浏览器会抛出 SSL 警告，要求用户在访问 FXOS 机箱之前接受证书。您必须使用 FXOS CLI

生成证书签名请求 (CSR) 并安装生成的身份证书，以便与 FXOS 机箱一起使用。此身份证书允许客户端浏览器信任连接，并直接启动 Web 界面而无警告。

有关安装受信任身份证书的完整程序，请参阅《思科 *FIREPOWER 4100/9300 FXOS CLI* 配置指南》中的“安装受信任身份证书”主题。

证书、密钥环和受信任点

HTTPS 使用公钥基础设施 (PKI) 的组件在两个设备（例如客户端浏览器和 Firepower 9300 机箱）之间建立安全通信。

加密密钥和密钥环

每个 PKI 设备具有一对非对称 Rivest-Shamir-Adleman (RSA) 加密密钥（其中一个保持为私有，另一个公开），存储在内部密钥环中。用任一密钥加密的消息均可用另一密钥解密。要发送加密消息，发送方使用接收方的公钥加密消息，接收方使用自己的私钥解密消息。发送方也可以通过使用其自有私钥加密（也称为“签名”）已知消息来证明其对公钥的所有权。如果接收方可使用上述公钥成功解密消息，则发送方对相应私钥的所有权得以证明。加密密钥长度可以不同，典型的长度为 512 位至 2048 位。一般来说，秘钥长度越长，安全性就越高。FXOS提供一个默认密钥环，带有 2048 位的初始密钥对，并允许创建更多密钥环。

如果群集名称更改或证书过期，则必须手动重新生成默认密钥环证书。

证书

作为安全通信前的准备，两台设备首先会交换数字证书。证书是包含设备的公钥以及有关设备身份的签名信息的文件。要仅支持加密通信，设备可生成自己的密钥对和自签名证书。远程用户连接至显示自签名证书的设备时，用户无法轻易验证设备身份，且用户浏览器最初会显示身份验证警告。默认情况下，FXOS 包含内置的自签名证书，其中包含来自默认密钥环的公钥。

受信任点

要为 FXOS 提供更强的身份验证，您可从受信任来源或信任点获取并安装确认设备身份的第三方证书。第三方证书由颁发证书的受信任点签署，该受信任点可以是根证书颁发机构 (CA)，也可以是中间 CA 或信任锚（通向根 CA 的信任链一部分）。要获取新证书，您必须通过 FXOS 生成证书请求，并将请求提交至受信任点。

重要事项 证书必须采用 Base64 编码 X.509 (CER) 格式。

配置 HTTPS

按照以下工作流程在 FXOS 机箱上配置和强化 HTTPS：

1. 创建密钥环（请参阅《思科 *FIREPOWER 4100/9300 FXOS CLI* 配置指南》中的“创建密钥环”主题）。
2. 为密钥链创建证书请求（请参阅《思科 *FIREPOWER 4100/9300 FXOS CLI* 配置指南》中的“使用高级选项为密钥环创建证书申请”主题）。
3. 创建受信任的点（请参阅《思科 *FIREPOWER 4100/9300 FXOS CLI* 配置指南》中的“创建受信任的点”主题）。
4. 将证书导入密钥环（请参阅《思科 *FIREPOWER 4100/9300 FXOS CLI* 配置指南》中的“将证书导入密钥环”主题）。

使用以下附加选项强化 HTTPS：

- 指定域使用的 Cipher Suite 安全级别 (**set https cipher-suite-mode**)。我们建议将值指定为 **strong** 或 **custom**。如果选择 custom，则必须指定域的 Cipher Suite 安全性自定义级别 (**set https cipher-suite** *cipher-suite-spec-string*)。
- 启用证书吊销列表检查。

配置 SSH

我们建议使用 SSHv2，默认情况下使用 TCP 端口 22 启用。请注意可在服务器和客户端上启用的以下 SSH 强化配置选项：

RSA 密钥强度 (set ssh-server host-key rsa/set ssh-client host-key rsa)

模数值（以位为单位）应为 8 的倍数，且介于 1024 到 2048 之间。指定的密钥模块大小越大，生成 RSA 密钥对所需的时间就越长。建议值为 2048。

加密算法 (set ssh-server encrypt-algorithm/set ssh-client encrypt-algorithm)

FXOS 支持以下加密算法：

```
3des-cbc    3DES  CBC
aes128-cbc  AES128 CBC
aes128-ctr  AES128 CTR
aes192-cbc  AES192 CBC
aes192-ctr  AES192 CTR
aes256-cbc  AES256 CBC
aes256-ctr  AES256 CTR
```

注释 3des-cbc 不符合通用标准。

Diffie-hellman 密钥交换算法 (set ssh-server kex-algorithm/set ssh-client kex-algorithm)

DH 密钥交换提供无法由任何一方单独确定的共享密钥。密钥交换与签名和主机密钥配合使用，以提供主机身份验证。此密钥交换方法提供显式服务器身份验证。有关使用 DH 密钥交换方法的详细信息，请参阅 RFC 4253。

FXOS 上支持以下 DH 算法：

```
diffie-hellman-group14-sha1  Diffie-Hellman Group14 SHA1
```

服务器和客户端 MAC 算法 (set ssh-server mac-algorithm/set ssh-client mac-algorithm)

FXOS 上支持以下 MAC 算法：

```
hmac-sha1      Hmac SHA1
hmac-sha2-256  HMAC SHA2 256
hmac-sha2-512  HMAC SHA2 512
```

密钥更新容量限制 (set ssh-server rekey-limit volume/set ssh-client rekey-limit volume)

确定 FXOS 断开会话连接之前连接上允许的流量（以 KB 为单位）。

密钥更新时间限制 (set ssh-server rekey-limit time/set ssh-client rekey-limit time)

确定 SSH 会话可以保持空闲状态的分钟数，之后 FXOS 会将会话断开。

设置严格主机密钥检查 (set ssh-client stricthostkeycheck)

控制 SSH 主机密钥检查：

- **启用** - 如果 FXOS 已知的主机文件中未包含主机密钥，连接将被拒绝。您必须在系统/服务范围内通过 FXOS CLI 命令 **enter ssh-host** 手动添加主机。
- **提示** - 对于机箱中未存储的主机密钥，系统会提示您是接受还是拒绝它。
- **禁用** -（默认）机箱将自动接受以前未存储的主机密钥。

有关在 FXOS 机箱上配置 SSH 的完整程序，请参阅《思科 *Firepower 4100/9300 FXOS* 机箱管理器配置指南》和《思科 *Firepower 4100/9300 FXOS CLI* 配置指南》中的“平台设置”章节。

保护 SNMP

正确保护 SNMP 的安全至关重要，因为只有这样，才能保护网络数据以及用于传输此类数据的网络设备的保密性、完整性和可用性。SNMP 提供有关网络设备运行状况的大量信息。必须保护此类信息，以免恶意用户利用这些数据攻击网络。

SNMPv3 同时提供了安全模型和安全级别。安全模型是为用户和用户所处的角色设置的身份验证策略。安全级别是安全模型中允许的安全级别。安全模型和安全级别相结合来确定在处理 SNMP 数据包时采用的安全机制。

SNMP 社区字符串是应用于 FXOS 机箱以限制对设备上 SNMP 数据的访问（只读和读写访问）的密码。应该像对待所有密码一样，仔细选择这些社区字符串，以确保它们不被轻松破解。应根据网络安全策略定期更改社区字符串。例如，当网络管理员更换职位或离开公司后，应更改此字符串。

有关 SNMP 安全模型和级别的受支持水平的更多信息，请参阅《思科 *FIREPOWER 4100/9300 FXOS CLI* 配置指南》中“平台设置”一章的“配置 SNMP”部分。

保护系统日志

系统日志记录是将来自设备的消息收集到运行系统日志后台守护程序的服务器的方法。将信息记录到中央系统日志服务器有助于汇聚日志和提醒。系统日志服务接受消息并将其存储在文件中，或者

根据简单配置文件打印消息。以这种形式记录日志可为日志提供受保护的长期存储。日志对常规故障排除及事件处理均有帮助。

将日志记录信息发送到远程系统日志服务器可以更有效地关联和审核跨网络设备的网络和安全事件。请注意，系统日志消息以明文形式传输。因此，网络针对管理流量提供的所有保护（例如，加密或带外访问）应扩展为包括系统日志流量。要确保系统日志流量永远不会通过不受信任的网络以明文形式发送，可以配置 IPSec 安全通道。IPSec 为通过公共网络的数据包提供端到端数据加密和身份验证服务。

有关如何在 FXOS 上配置系统日志的详细信息，请参阅《思科 *FIREPOWER 4100/9300 FXOS CLI* 配置指南》中“平台设置”一章的配置系统日志部分。有关如何配置 IPSec 的详细信息，请参阅《思科 Firepower 4100/9300 FXOS CLI 配置指南》中的配置 *IPSec* 安全通道主题。

配置 IP 访问列表

默认情况下，FXOS 机箱会拒绝对本地 Web 服务器的所有访问。您必须使用每个协议允许的主机或子网的 IP 地址配置 IP 访问列表。

IP 访问列表支持以下协议：

- HTTPS
- SSH
- SNMP

对于每个 IP 地址列表（v4 或 v6），可以为每项服务配置最多 100 个不同的子网。子网 0 和前缀 0 允许无限制无限访问服务。

有关在 FXOS 机箱上配置 IP 访问列表的详细信息和完整程序，请参阅《思科 *Firepower 4100/9300 FXOS* 机箱管理器配置指南》和《思科 *Firepower 4100/9300 FXOS CLI* 配置指南》中“平台设置”章节的“配置 IP 访问列表”主题。

配置 IPSec 安全通道

在 Firepower 4100/9300 机箱上配置 IPSec，可对通过公用网络的数据包提供端到端的数据加密和身份验证服务。

注释　如果您在 FIPS 模式下使用 IPSec 安全通道，则 IPSec 对等体必须支持 RFC 7427。

有关如何为 FXOS 机箱配置 IPSec 安全通道的完整说明，请参阅《思科 *Firepower 4100/9300 FXOS CLI* 配置指南中“安全认证合规性”一章中的“配置 IPSec 安全通道”主题。

关于证书撤销吊销列表检查

您可以在 IPSec、HTTPS 和安全 LDAP 连接中将证书吊销列表 (CRL) 检查模式配置为“严格”或“宽松”。

FXOS 从 X.509 证书的 CDP 信息中获取动态（非静态）CRL 信息，该信息指示动态 CRL 信息。系统管理人员会手动下载指示 FXOS 系统中的本地 CRL 信息的静态 CRL 信息。FXOS 根据证书链中当前正在处理的证书处理动态 CRL 信息。静态 CRL 信息则应用于整个对等证书链。

有关启用或禁用对安全 IPSec、LDAP 和 HTTPS 连接的证书吊销检查的具体步骤，请参阅配置 IPSec 安全通道、创建 LDAP 提供程序和配置 HTTPS。

注释

- 如果“证书撤销检查模式 (Certificate Revocation Check Mode)”设置为“严格 (Strict)”，则仅当对等证书链具有级别 1 或更高级别时，静态 CRL 才适用。（例如，当对等证书链仅包含根 CA 证书和根 CA 签名的对等证书时。）
- 为 IPSec 配置静态 CRL 时，导入的 CRL 文件中必须具有“授权密钥标识符 (authkey) (Authority Key Identifier [authkey])”字段。否则，IPSec 会将其视为无效。
- 静态 CRL 优先于来自同一颁发者的动态 CRL。当 FXOS 验证对等证书时，如果存在同一颁发者的有效（已确定）静态 CRL，FXOS 会忽略对等证书中的 CDP。
- 默认在以下场景中启用严格 CRL 检查：
  - 新创建的安全 LDAP 提供程序连接、IPSec 连接或客户端证书条目
  - 新部署的 FXOS 机箱管理器（使用 FXOS 2.3.1.x 或更高版本的初始启动版本部署）

下表说明了连接结果，具体取决于证书吊销列表检查设置和证书验证。

表 *1:* 无本地静态 *CRL* 时将“证书撤销检查模式 *(Certificate Revocation Check Mode)*”设置为“严格 *(Strict)*”

无本地静态 CRL	LDAP 连接	IPSec 连接	客户端证书身份验证
检查对等证书链	需要完整的证书链	需要完整的证书链	需要完整的证书链
检查对等证书链中的 CDP	需要完整的证书链	需要完整的证书链	需要完整的证书链
针对对等证书链的根CA证书执行 CDP 检查	是	不适用	是
对等证书链中的任何证书验证失败	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
在对等证书链中撤销了任何证书	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息

无本地静态 CRL	LDAP 连接	IPSec 连接	客户端证书身份验证
对等证书链中缺少一个 CDP	连接失败，系统显示系统日志消息	对等证书：连接失败，系统显示系统日志消息 中间 CA：连接失败	连接失败，系统显示系统日志消息
某个 CDP CRL 在具有有效签名的对等证书链中为空	连接成功	连接成功	连接失败，系统显示系统日志消息
无法下载对等证书链中的任何 CDP	连接失败，系统显示系统日志消息	对等证书：连接失败，系统显示系统日志消息 中间 CA：连接失败	连接失败，系统显示系统日志消息
证书具有 CDP，但 CDP 服务器已关闭	连接失败，系统显示系统日志消息	对等证书：连接失败，系统显示系统日志消息 中间 CA：连接失败	连接失败，系统显示系统日志消息
证书具有 CDP，服务器已启动且 CRL 在 CDP 上具有 CRL，但 CRL 具有无效签名	连接失败，系统显示系统日志消息	对等证书：连接失败，系统显示系统日志消息 中间 CA：连接失败	连接失败，系统显示系统日志消息

表 *2:* 具有本地静态 *CRL* 时将“证书撤销检查模式 *(Certificate Revocation Check Mode)*”设置为“严格 *(Strict)*”

具有本地静态 CRL	LDAP 连接	IPSec 连接
检查对等证书链	需要完整的证书链	需要完整的证书链
检查对等证书链中的 CDP	需要完整的证书链	需要完整的证书链
针对对等证书链的根 CA 证书执行 CDP 检查	是	不适用
对等证书链中的任何证书验证失败	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
在对等证书链中撤销了任何证书	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
对等证书链中缺少一个 CDP（证书链级别为 1）	连接成功	连接成功
对等证书链中的一个 CDP CRL 为空（证书链级别为 1）	连接成功	连接成功
无法下载对等证书链中的任何 CDP（证书链级别为 1）	连接成功	连接成功

具有本地静态 CRL	LDAP 连接	IPSec 连接
证书具有 CDP，但 CDP 服务器已关闭（证书链级别为 1）	连接成功	连接成功
证书具有CDP，服务器已启动且 CRL 在 CDP 上，但 CRL 具有无效签名（证书链级别为 1）	连接成功	连接成功
对等证书链级别高于 1	连接失败，系统显示系统日志消息	如果与 CDP 结合，连接会成功 如果没有CDP，连接会失败并生成系统日志消息

表 *3:* 无本地静态 *CRL* 时将“证书撤销检查模式 *(Certificate Revocation Check Mode)*”设置为“释放 *(Relaxed)*”

无本地静态 CRL	LDAP 连接	IPSec 连接	客户端证书身份验证
检查对等证书链	完整的证书链	完整的证书链	完整的证书链
检查对等证书链中的 CDP	完整的证书链	完整的证书链	完整的证书链
针对对等证书链的根CA证书执行 CDP 检查	是	不适用	是
对等证书链中的任何证书验证失败	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
在对等证书链中撤销了任何证书	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
对等证书链中缺少一个 CDP	连接成功	连接成功	连接失败，系统显示系统日志消息
某个CDP CRL 在具有有效签名的对等证书链中为空	连接成功	连接成功	连接成功
无法下载对等证书链中的任何 CDP	连接成功	连接成功	连接成功
证书具有CDP，但CDP服务器已关闭	连接成功	连接成功	连接成功
证书具有 CDP，服务器已启动且 CRL 在 CDP 上，但CRL 具有无效签名	连接成功	连接成功	连接成功

表 *4:* 具有本地静态 *CRL* 时将“证书撤销检查模式 *(Certificate Revocation Check Mode)*”设置为“释放 *(Relaxed)*”

具有本地静态 CRL	LDAP 连接	IPSec 连接
检查对等证书链	完整的证书链	完整的证书链
检查对等证书链中的 CDP	完整的证书链	完整的证书链
针对对等证书链的根 CA 证书执行 CDP 检查	是	不适用
对等证书链中的任何证书验证失败	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
在对等证书链中撤销了任何证书	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
对等证书链中缺少一个CDP（证书链级别为 1）	连接成功	连接成功
对等证书链中的一个 CDP CRL 为空（证书链级别为 1）	连接成功	连接成功
无法下载对等证书链中的任何 CDP（证书链级别为 1）	连接成功	连接成功
证书具有 CDP，但 CDP 服务器已关闭（证书链级别为 1）	连接成功	连接成功
证书具有CDP，服务器已启动且 CRL 在 CDP 上，但 CRL 具有无效签名（证书链级别为 1）	连接成功	连接成功
对等证书链级别高于 1	连接失败，系统显示系统日志消息	如果与 CDP 结合，连接会成功 如果没有CDP，连接会失败并生成系统日志消息

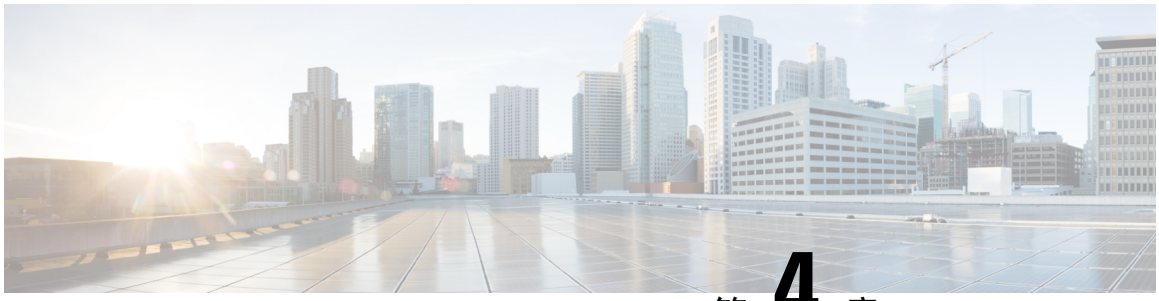
配置信任点静态 CRL

已吊销证书保留在证书吊销列表 (CRL) 中。客户端应用使用 CRL 检查服务器的身份验证。服务器应用利用 CRL 授予或拒绝来自不再受信任的客户端应用的访问请求。

您可以配置 Firepower 4100/9300 机箱以使用证书吊销列表 (CRL) 信息验证对等证书。

配置为使用证书吊销列表信息验证对等证书后，还可以将系统配置为定期下载 CRL，以便每隔 1 到 24 小时使用一个新的 CRL 来验证证书。

有关如何为信任点配置证书吊销列表的详细说明，请参阅《思科 *FIREPOWER 4100/9300 FXOS CLI* 配置指南》中“安全认证合规性”一章的“为信任点配置静态 CRL”主题。



第 4 章

保护基于角色的访问控制

系统为用户角色分配了权限，用于定义用户可以在系统上执行的操作。系统包含以下用户角色：

管理员

完成对整个系统的读写访问。默认情况下，此角色分配给默认的管理员帐户，并且不能对其进行更改。

只读

对系统配置进行只读访问，但无权修改系统状态。

运营

对NTP配置、用于智能许可的Smart Call Home配置和系统日志（包括系统日志服务器和故障）进行读写访问。对系统其余部分的读取访问。

AAA 管理员

对用户、角色和 AAA 配置的读写访问。对系统其余部分的读取访问。

通过 FXOS 机箱管理器 Web 界面或 FXOS CLI，您可以为系统中的每个用户帐户配置以下设置：

- User Role - 表示要分配给用户帐户的权限的角色。

  所有用户均默认分配了 Read-Only 角色，并且此角色无法取消选择。要分配多个角色，请按住 **Ctrl** 键并单击所需的角色。

- Account Expiration Date
- Account Status - 如果状态设置为**活动**，用户可以使用其登录 ID 和密码登录到 Firepower 机箱管理器和 FXOS CLI。

为了让经过本地身份验证的帐户获得最高的安全性，请为加密会话配置 SSH。

- 密码管理，第 20 页
- 强化经过本地身份验证的用户帐户，第 20 页
- 强化经过远程身份验证的用户帐户，第 20 页

密码管理

密码控制对资源或设备的访问，管理员定义密码以验证请求。当 FXOS 收到访问资源或设备的请求时，系统会质询请求并验证密码和身份，然后根据结果授予、拒绝或限制访问权限。最佳安全时间要求使用 LDAP、TACACS+ 或 RADIUS 身份验证服务器管理密码。但是，如果 LDAP、TACACS+ 或 RADIUS 服务出现问题，仍然需要本地配置的访问密码。设备还可以在其配置中包含其他密码信息，例如 NTP 密钥或 SNMP 社区字符串。

强化经过本地身份验证的用户帐户

配置单个内部用户角色时，管理员帐户用户可以使用以下设置通过 Web 界面登录机制强化系统以抵御攻击：

- 设置允许用户尝试登录的最大失败次数，如果超过该次数，用户会被锁定一段指定的时间 (**set max-login-attempts**)
- 设置在超出最大尝试登录次数后用户应被系统锁定的时间 (**set user-account-unlock-time**)
- 实施最小密码长度 (**set min-password-length**)
- 指定经过本地身份验证的用户在更改新建密码之前必须等待的最少小时数 (**set no-change-interval**)
- 设置本地用户帐户有效的天数 (**set expiration**)
- 需要强密码 (**set enforce-strong-password yes**)
- 分配仅适用于用户所需访问类型的用户访问权限 (**create role**)

强化经过远程身份验证的用户帐户

远程身份验证的用户账户是指任何通过 LDAP、RADIUS 或 TACACS+ 进行身份验证的用户账户。远程身份验证最多允许 16 个 TACACS+ 服务器、16 个 RADIUS 服务器和 16 个 LDAP 提供程序，共计 48 个提供程序。

AAA 是一组服务，用于控制对计算机资源的访问、实施策略、评估使用情况并提供对服务进行计费所需的信息。这些过程对于高效进行网络管理和安全性而言至关重要。

请注意，如果用户同时持有本地用户帐户和远程用户帐户，则在本地用户帐户中定义的角色将覆盖在远程用户帐户中持有的角色。

TACACS+ 是 FXOS 机箱可用来对远程 AAA 服务器进行管理用户身份验证的身份验证协议。这些管理用户可以通过 SSH、HTTPS、telnet 或 HTTP 访问 FXOS 机箱。我们建议使用 SSH 以便在访问 FXOS 机箱时获得最大的安全性。许多身份验证方法提供增强的安全性。

TACACS+ 验证（或者更通用的 AAA 身份验证）使得每个网络管理员可以使用一个用户帐户。当您不依赖单个共享的密码时，网络的安全性会得到改善，您的问责制度也会得到加强。

RADIUS 是用途与 TACACS+ 类似的协议；但是，其仅加密网络中发送的密码。相反，TACACS+ 则为整个 TCP 负载（包括用户名和密码）加密。因此，我们建议您在 AAA 服务器支持 TACACS+ 时，优先使用 TACACS+。

LDAP 是用于访问目录服务的客户端-服务器协议，例如 Microsoft Active Directory。LDAP 对于客户端与服务器之间的安全性没有要求。但是，如果使用 SSL，LDAP 可以将客户端与服务器之间的用户会话加密。这样可保证在网络上的 LDAP 事务中传输的所有信息安全。因此，我们强烈建议您优先使用 LDAP 而非 TLS。

有关如何在 FXOS 机箱上配置 RADIUS、TACAS+ 和 LDAP 的详细信息和详细程序，请参阅《思科 *FIREPOWER 4100/9300 FXOS CLI* 配置指南》中“平台设置”一章的配置 AAA 部分。

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。