



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，第 1 页](#)
- [控制和加密管理会话，第 2 页](#)
- [安装受信任身份证书，第 2 页](#)
- [证书、密钥环和受信任点，第 3 页](#)
- [配置 HTTPS，第 3 页](#)
- [配置 SSH，第 4 页](#)
- [保护 SNMP，第 5 页](#)
- [保护系统日志，第 5 页](#)
- [配置 IP 访问列表，第 6 页](#)
- [配置 IPSec 安全通道，第 6 页](#)
- [关于证书撤销吊销列表检查，第 7 页](#)
- [配置信任点静态 CRL，第 10 页](#)

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，密钥长度越长，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。

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。