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。

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。