Secure Network Operations

Securing network operations is a substantial topic. Although most of this document is devoted to the secure configuration of a Firepower 4100/9300 device running FXOS, configurations alone do not completely secure a network. The operational procedures in use on the network, as well as the people who administer the network, contribute as much to security as the configuration of the underlying devices.

The following sections contain operational recommendations that FXOS administrators are advised to implement. These sections highlight specific critical areas of network operations and are not comprehensive.

Monitor Cisco Security Advisories

The Cisco Product Security Incident Response Team (PSIRT) creates and maintains publications, commonly referred to as Cisco Security Advisories, for security-related issues in Cisco products. Security advisories are available at http://www.cisco.com/go/psirt.

For information about Cisco PSIRT vulnerability reporting, see the Cisco Security Vulnerability Policy.

To maintain a secure system, Cisco FXOS administrators should be aware of the information communicated in Cisco Security Advisories. Detailed knowledge of the vulnerability is required before evaluating the threat that the vulnerability can pose to a network. For assistance with this evaluation process, see Risk Triage for Security Vulnerability Announcements.

Update to Latest Version of FXOS

Important security updates are included in each new platform bundle release of FXOS. We recommend you update your FXOS system to the latest available version as soon as possible.

For more information on supported compatibility and upgrade paths for FXOS in various configurations, see the *Cisco Firepower 4100/9300 FXOS Compatibility* guide and the *Cisco Firepower 4100/9300 Upgrade Guide* on Cisco.com.

Customize the Pre-Login Banner

You can specify the message that FXOS displays to users before they log into Firepower Chassis Manager or the FXOS CLI. From a hardening perspective, this message should be used to discourage unauthorized access.

The following CLI example creates a pre-login banner for the FXOS Chassis Manager and FXOS CLI:

```
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 #
```

Enable Common Criteria or FIPS Mode

If your organization is required to use only equipment and software that comply with security standards established by the U.S. Department of Defense or other governmental certification organizations, you can enable Common Criteria or FIPS mode to apply multiple hardening changes with a single setting. Note that if your organization is not required to comply with security certifications compliance standards, you may still enable FIPS or Common Criteria modes for FXOS, but be aware that this may cause compatibility issues on your device.

The options to enable Common Criteria or FIPS mode appear under **Platform Settings** > **FIPS/Common Criteria** mode in the Firepower Chassis Manager web interface.

Note

- Enabling security certifications compliance does not guarantee strict compliance with all requirements of the security mode selected. Additional settings recommended to harden your deployment above and beyond those provided by Common Criteria or FIPS modes are described in this document. For full information on hardening procedures required for complete compliance, refer to the guidelines for this product provided by the certifying entity.
- Use FIPS compliant tool for device access when FIPS, Common Criteria, or both are enabled.

Secure the Network Time Protocol (NTP)

We strongly recommend using a trusted Network Time Protocol (NTP) server to synchronize system time on your Firepower 4100/9300 FXOS device and its associated servers.

To enable NTP for FXOS, you must first generate NTP key IDs and key values, then add the NTP server to the FXOS chassis using the following workflow in FXOS Chassis Manager: **Platform Settings > Set Time Source > Use NTP Server**. To further harden NTP, configure NTP server authentication.

For full instructions on how to configure an NTP server and NTP server authentication for FXOS, see the Setting the Date and Time Using NTP topic of the Platform Settings chapter in the *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*.

Note

- When enabled, the NTP authentication feature is global for all configured servers associated with FXOS.
- Only SHA1 is supported for NTP server authentication.
- You need the key ID and the key value to authenticate a server. The key ID is used to tell both the client and server which key value to use when computing the message digest. The key value is a fixed value that is derived using nip-keygen.

Secure the Domain Name System (DNS)

Computers communicating with each other in a networked environment depend on the DNS protocol to provide mapping between IP addresses and host names.

DNS can be susceptible to specific types of attacks tailored to take advantage of weak points in a DNS server that is not configured with security in mind. Be sure your local DNS server is configured in keeping with industry-recommended best practices for security; Cisco offers guidelines in this document: https://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html.

Leverage Authentication, Authorization, and Accounting

The Authentication, Authorization, and Accounting (AAA) framework is critical to securing interactive access to network devices. The AAA framework provides a highly configurable environment that can be tailored based on the needs of the network.

RADIUS and TACACS+ are both supported on the FXOS system. TACACS+ encrypts the entire TCP payload, which includes both the username and password. Radius encrypts only the password. Additionally, TACACS+ provides for command authorization, whereas RADIUS only provides authentication and accounting. Therefore, we suggest you use TACACS+ for maximum authentication security.

Additionally, you can use LDAP for user authentication. To encrypt the LDAP authentication exchange, use the CLI option to use SSL.

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

For more information and complete procedures on how to configure AAA, see the "Configuring AAA" section of the Platform Settings chapter in the *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*.

Use Secure Protocols

Cisco FXOS uses many protocols in order to carry sensitive network management data. You must use secure protocols whenever possible. A secure protocol choice includes the use of SSH instead of Telnet so that both authentication data and management information are encrypted. In addition, you must use secure file transfer protocols when you copy configuration data. For example, the use of Secure Copy Protocol (SCP) in place of FTP or TFTP. For additional details on how to use secure protocols, see the Management Plane section of this document.

Configuration Management

Configuration management is a process by which configuration changes are proposed, reviewed, approved, and deployed.

The configuration of a Cisco FXOS device contains many sensitive details, including usernames, passwords, and the contents of access control lists (ACLs). The repository used to archive Cisco FXOS device configurations should be secured and access should be restricted to only those roles and functions that require access. Insecure access to this information can undermine the security of the entire network.