# Introduction

This document provides information to help you harden your Cisco Firepower eXtensible Operating System (FXOS) on 4100 and 9300 platform devices, which increases the overall security of your network. For hardening information on other components of your Firepower deployment, see the following documents:

- Cisco Guide to Harden ASA Firewall
- Cisco Firepower Management Center Hardening Guide, Version 6.4
- Cisco Firepower Threat Defense Hardening Guide, Version 6.4

The three functional planes of a network - the management, control, and data planes, each provide a different functionality that must be protected.

**Management Plane**

The management plane contains the logical group of all traffic that supports provisioning, maintenance, and monitoring functions for Cisco FXOS. Traffic in this group includes HTTP/HTTPS, SSH, FTP, Simple Network Management Protocol (SNMP), Syslog, TACACS+, Remote Authentication Dial-In User Service (RADIUS), and DNS. Management plane traffic is always destined to the local Cisco FXOS.

**Control Plane**

The control plane contains the logical group of all switching, signaling, link-state, and other control protocols that are used to create and maintain the state of the network and interfaces such as Link Layer Discovery Protocol (LLDP), and Link Aggregation Control Protocol (LACP). Control plane traffic is always destined to the local Cisco FXOS device.

**Data Plane**

The data plane contains the logical group of customer application traffic generated by hosts, clients, servers, and applications that are sourced from and destined to other similar devices supported by the network.

This document is structured in three sections:

- Secure Network Operations
- Management Plane Hardening
- User Management

Although most of this document is devoted to secure configuration of a Cisco FXOS device, 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. Where possible and appropriate, this document contains recommendations that, if implemented, help secure a Cisco FXOS deployment.

# Security Certifications Compliance

Note that your organization might be 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.

When configured in accordance with certification-specific guidance documents the Firepower System supports compliance with the following certification standards:

- Common Criteria (CC): a global standard established by the international Common Criteria Recognition Arrangement, defining requirements for security products.
- Department of Defense Information Network Approved Products List (DoDIN APL): a list of products meeting security requirements established by the U.S. Defense Information Systems Agency (DISA). NOTE: The U.S. Government has changed the name of the Unified Capabilities Approved Products List (UCAPL) to the DoDIN APL. References to UCAPL in Firepower documentation and the Firepower Management Center web interface can be interpreted as references to DoDIN APL.
- Federal Information Processing Standards (FIPS) 140: a requirements specification for encryption modules.

Certification guidance documents are available separately once product certifications have completed; publication of this hardening guide does not guarantee completion of any of these product certifications.