cyber.encse

CIS CISCO IOS BENCHMARK — ALIGNED

Cisco IOS Security Hardening Guide

Management plane, control plane, and data plane hardening for Cisco IOS/IOS-XE devices, with sample configurations.

This guide provides hardening rationale and verification commands for a security baseline. Always test in a non-production environment first — some settings can break application compatibility or legacy integrations. Not every control applies to every environment; assess against your own risk tolerance.

Published by eNeoteric Consultancy Services · cyber.encse.com · v1.0, August 2026

1. Management Plane Hardening

1.1 Disable unused management services

```
no service pad
no ip source-route
no ip finger
no service finger
no ip http server
no ip http secure-server
no service config
no cdp run
no ip bootp server
```

CDP and unnecessary HTTP/finger services leak topology and device information to anyone on the local segment, and each open service is additional attack surface with no operational benefit on most devices.

1.2 Secure remote access — SSH only, disable Telnet

```
ip domain-name example.com
crypto key generate rsa modulus 2048
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 3

line vty 0 15
transport input ssh
exec-timeout 10 0
login local
```

Telnet transmits credentials and session data in cleartext. Restricting to SSHv2 with a 2048-bit (or larger) RSA key closes off trivial network eavesdropping and credential theft on the management plane.

1.3 Restrict management access by source

```
access-list 10 permit 10.0.0.0 0.255.255.255
access-list 10 deny any log

line vty 0 15
access-class 10 in
```

Management interfaces (SSH, HTTP(S), SNMP) should never be reachable from untrusted networks — restrict to a dedicated management VLAN or jump host range.

2. AAA & Authentication

```
aaa new-model
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+

username admin-local privilege 15 secret <STRONG_PASSWORD>
enable secret <STRONG_PASSWORD>
no enable password
```

Centralised AAA (TACACS+/RADIUS) provides individual accountability and rapid access revocation across the fleet; the local account remains as a fallback if the AAA server is unreachable. `enable secret` uses a stronger hash than the deprecated `enable password`.

2.1 Password policy

```
security passwords min-length 12
login block-for 120 attempts 5 within 60
login delay 2
```

`login block-for` throttles brute-force login attempts by blocking further attempts fleet-wide after repeated failures within a window.

3. Control Plane Protection

- Enable Control Plane Policing (CoPP) to rate-limit traffic destined to the router's own control plane, protecting against control-plane DoS.
- Disable IP source routing and directed broadcasts (smurf attack mitigation) — `no ip directed-broadcast` per interface.
- Enable uRPF (Unicast Reverse Path Forwarding) on edge interfaces to drop spoofed-source traffic.
- Disable unused physical and logical interfaces (`shutdown`) to reduce the exposed attack surface.

```
interface GigabitEthernet0/1
ip verify unicast source reachable-via rx
no ip directed-broadcast
no ip proxy-arp
```

4. Logging & Monitoring

```
logging buffered 16384 informational
logging trap informational
logging source-interface Loopback0
logging host 10.0.0.50
service timestamps log datetime msec localtime show-timezone
ntp server 10.0.0.10
ntp server 10.0.0.11
```

Accurate, synchronised timestamps (NTP) are essential for correlating device logs with other security telemetry during an investigation. Forward logs to a central syslog/SIEM collector — local buffered logs are lost on reload.

4.1 SNMP — use v3 only, or disable

```
no snmp-server community public
no snmp-server community private
snmp-server group SECGROUP v3 priv
snmp-server user secadmin SECGROUP v3 auth sha <AUTH_PASS> priv aes 128 <PRIV_PASS>
```

SNMPv1/v2c community strings are transmitted in cleartext and are frequently left at default values ("public"/"private") — a very common finding in penetration tests. SNMPv3 provides authentication and encryption.

5. Data Plane / ACL Hygiene

- Apply anti-spoofing ACLs (RFC 2827/BCP 38) at network edges — block traffic with source addresses from your own internal ranges arriving on external interfaces.
- Explicitly deny and log traffic to RFC 1918 / bogon source addresses on internet-facing interfaces.
- Review ACLs at least annually for unused/overly-permissive rules — ACL sprawl is a common source of unintended exposure.
- Use named ACLs with descriptive remarks for auditability, not unlabelled numbered ACLs.

6. Patch & Version Management

- Track Cisco PSIRT advisories for your deployed IOS/IOS-XE versions; prioritise any CVE listed in CISA's Known Exploited Vulnerabilities (KEV) catalog.
- Run a currently-supported IOS/IOS-XE release — end-of-life versions no longer receive security fixes.
- Validate `show version` against your asset inventory quarterly to catch unauthorised/uncoordinated firmware changes.
- Maintain offline, hashed backups of running-config and startup-config for rapid, verified recovery.

7. Verification Checklist

Control	Verified
Telnet disabled, SSHv2-only with 2048-bit+ RSA key	
Unused services disabled (CDP, HTTP server, finger, PAD)	
Management access restricted by source ACL (access-class)	
AAA (TACACS+/RADIUS) configured with local fallback	
enable secret used (not enable password); min password length enforced	
login block-for configured against brute-force	
Control Plane Policing (CoPP) and uRPF enabled on edge interfaces	
Syslog forwarded to central collector; NTP synchronised	
SNMPv3 only (or SNMP disabled) — no v1/v2c community strings	
Anti-spoofing / BCP 38 ACLs applied at network edges	
Running a currently-supported, patched IOS/IOS-XE version	

Based on the CIS Cisco IOS Benchmark. Sample configurations are illustrative — validate syntax against your specific IOS/IOS-XE version and test in a lab before applying to production network infrastructure.