Cisco CCNP Security (350-701 SCOR) Commands Sheet

Practical commands for logging, AAA, VPN checks, traffic validation, and security operations.

Best for	Focus	Use with
Command recall before labs and review sessions	What each command does and when to use it	Use with ports sheet and cheat sheet

1. Core checks

show logging	Review recent device and security events.
show running-config	Confirm actual configuration before assuming.
show access-lists	Validate rule order and hit counts.
show clock detail	Time problems can break logs, certs, and auth assumptions.

2. Access and identity

show aaa servers	Validate AAA back-end visibility on supported platforms.
show authentication sessions	Check 802.1X / session state on supported switches.
test aaa group	Useful for validating AAA policy paths on supported devices.
show users	See active management sessions.

3. VPN and crypto awareness

show crypto isakmp sa	Legacy IKE Phase 1 state on supported platforms.
show crypto ikev2 sa	Check IKEv2 session establishment.
show crypto ipsec sa	Verify data-plane IPsec state and counters.
show vpn-sessiondb	Useful on ASA/FTD contexts for remote-access sessions.

4. Traffic and packet visibility

packet-tracer	ASA-style simulated packet path validation.
capture / monitor capture	On-box capture options on supported security gear.
tcpdump	Packet capture on Linux-like platforms.
curl -I URL	Quick HTTPS/header test during policy troubleshooting.

5. Practical reminders

Logs + counters + captures	Use all three before concluding root cause.
Secure replacements	Prefer SSH, HTTPS, LDAPS, and SNMPv3 over older plaintext options.
Identity-aware security	Know which tools answer user, device, posture, and session questions.
Rollback matters	In security changes, a safe rollback path is part of the answer.