

Cisco CCNP Security (350-701 SCOR) Quick Summary

Fast 3-5 minute refresh for the core SCOR themes, comparisons, and common traps.

Best for Ultra-fast memory refresh	Focus Definitions, priorities, and security shortcuts	Use with Use with cheat sheet for deeper review
--	---	---

1. Fast refresh

SCOR scope	Network security, cloud security, content security, endpoint protection and detection, secure access, visibility, enforcements.
Think layered	The best control set is usually identity + segmentation + monitoring, not a single product.
Visibility first	If you cannot see the event, you cannot defend it well.
Policy over plumbing	Many questions are really about policy intent and enforcement points.

2. Common traps

RADIUS vs TACACS+	Access control for network entry versus classic device administration use cases.
Detection vs prevention	Seeing bad activity is not the same as stopping it.
VPN vs ZTNA style access	Do not assume every remote access problem wants the same answer.
TLS inspection limits	Inspection improves visibility but can break things or add operational cost.

3. Security shortcuts

Least privilege	Apply it to users, devices, services, and network paths.
MFA	High-value protection for many access paths.
Segmentation	Improves both containment and policy clarity.
Logging	Security answers without log visibility are usually incomplete.

4. Ops shortcuts

Syslog	Event trail.
NetFlow / telemetry	Traffic visibility.
AAA accounting	Who did what.
Packet capture	Ground truth when guesses fail.