Cisco CCNP Security (350-701 SCOR) Cheat Sheet

One-page cram sheet for network security, cloud/content security, endpoint protection, secure access, visibility, and operations.

Best for	Focus	Use with
Last review before drills or exam day	Security layers + policy intent + visibility flow	Use with ports sheet and commands sheet

1. Network security

Segmentation	Use firewalls, VRFs, ACLs, zones, and trust boundaries to limit blast radius and enforce policy.
Secure management	SSH, AAA, RBAC, logging, and encrypted management protocols are expected defaults.
VPN foundations	Know remote access vs site-to-site, IPsec building blocks, and why NAT-T matters.
Policy enforcement	The best answer often combines identity, device posture, and path control rather than one box alone.

2. Cloud and content security

Shared responsibility	The provider secures parts of the stack; the customer still owns identity, data, config, and monitoring decisions.
Content controls	Email/web/content security questions focus on inspection, filtering, malware defense, and DLP-style enforcement.
TLS inspection tradeoffs	Great for visibility, but it adds privacy, certificate, and performance considerations.
Proxy thinking	Forward/reverse proxy use cases still matter in secure web and access designs.

3. Endpoint protection and detection

EDR/XDR concepts	Know prevention vs detection vs response and why telemetry quality matters.
Endpoint posture	Compliance checks, agent state, encryption, and patch level can drive access decisions.
Threat visibility	Security tools are strongest when they correlate endpoint, network, identity, and log data.
Containment	Isolation is often the right early move while investigation continues.

4. Secure network access + visibility

AAA	RADIUS/TACACS+, identity stores, authorization policy, and accounting appear frequently.

802.1X / posture	User and device context can decide if access is granted, limited, or quarantined.
Logs + telemetry	Syslog, flow data, alarms, and packet captures each answer different questions.
Zero Trust mindset	Verify explicitly, minimize trust, and assume compromise.

5. Automation and operations

APIs + automation	Security operations increasingly use APIs, JSON, and templates for consistency and speed.
Change validation	Validate intended state, rollback plan, and monitoring before broad rollout.
Incident flow	Identify, contain, eradicate, recover, and review.
Security outcomes	Prefer answers that improve visibility and enforce least privilege with manageable operations.