CCNP SECURITY · CCIE SECURITY

SCOR
350-701

Complete Learning Guide

EXAM VERSION v2.0

Independent · Unofficial Study Guide

JOZEF BAROŠ

SCOR 350-701 v2.0

Complete Learning Guide

Implementing and Operating Cisco Security Core Technologies v2.0

For the **350-701 SCOR v2.0** exam blueprint — the version of the exam delivered from **27 August 2026**. This book does not cover the retired v1.1 blueprint.

An independent, unofficial study guide for the CCNP Security and CCIE Security certifications.

6 domains · 47 topics · 235 questions · 34 diagrams

Worked examples · Field scenarios · Exam tips · Glossary · v1.1 → v2.0 change appendix

Copyright, Trademarks, and Disclaimer

Independent and unofficial

This book is an independent publication. It is not affiliated with, authorised by, sponsored by, endorsed by, or otherwise approved by Cisco Systems, Inc. The author is not employed by, and has no commercial relationship with, Cisco Systems, Inc. in connection with this publication.

Cisco does not review, license, or certify third-party study materials, and no statement in this book should be read as a representation by Cisco. Where this book describes the behaviour of a Cisco product, it does so as independent technical commentary.

Trademarks

Cisco, the Cisco logo, Cisco Systems, CCNA, CCNP, CCIE, Cisco Secure Firewall, Firepower, Cisco Identity Services Engine (ISE), Cisco Secure Endpoint, Cisco Secure Client, AnyConnect, Cisco Secure Access, Umbrella, Cisco Secure Malware Analytics, Cisco Secure Workload, Cisco Multicloud Defense, Cisco Secure Network Analytics, Stealthwatch, Cisco XDR, Duo, pxGrid, TrustSec, Talos, and SAFE are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Splunk and Splunk Enterprise Security are trademarks or registered trademarks of Splunk Inc. Microsoft, Microsoft 365, Windows, PowerShell, and Azure are trademarks of Microsoft Corporation. MITRE ATT&CK is a registered trademark of The MITRE Corporation. All other trademarks, service marks, and trade names referenced in this book are the property of their respective owners.

All product names, logos, and brands are used for identification and educational purposes only. Their use does not imply endorsement, affiliation, or any commercial relationship. No Cisco copyrighted material, courseware, exam content, or product documentation has been

reproduced in this book; all explanations, diagrams, configurations, and questions are original work by the author.

No exam content

This book contains no actual examination questions and no material obtained from any Cisco examination. The practice questions in this book were written by the author to illustrate the concepts in each topic. Using or distributing real examination content — commonly called a braindump — violates the Cisco Certifications and Confidentiality Agreement and can result in permanent decertification. If you encounter material claiming to contain real exam questions, do not use it.

Accuracy, currency, and liability

This book is written against the **350-701 SCOR v2.0 exam blueprint**, first delivered on 27 August 2026. Cisco states that exam topics may change at any time without notice, and product interfaces, feature names, and default behaviours change frequently. **Always verify the current blueprint at Cisco's official certification pages before you book your exam**, and treat any configuration in this book as an illustration to be adapted, not a template to be pasted into production.

The information in this book is provided on an “as is” basis, without warranty of any kind, express or implied. Neither the author nor the publisher shall be liable for any loss, damage, service interruption, security incident, or exam outcome arising directly or indirectly from the use of this material. Configuration examples are for study purposes; test them in a laboratory environment before applying anything to a production network.

Passing any certification exam depends on your own preparation and experience. No book can guarantee a result, and this one does not attempt to.

Contact and errata

Corrections, questions, and feedback are genuinely welcome and improve later editions. Please contact the author through the storefront where you purchased this book.

About This Book

In August 2026 Cisco replaced the SCOR 350-701 v1.1 blueprint with **v2.0**, and it is not a light refresh. An entire domain — Secure Service Edge — is new. Artificial intelligence appears twice: once as a category of threat and once as a category of vulnerability in the models organisations now deploy themselves. Post-quantum cryptography, QUIC, and MASQUE join the cryptography topic. Splunk appears three times. Meanwhile a great deal of appliance-era detail has quietly disappeared.

That combination creates a problem for anyone preparing today: **most of the study material in circulation was written for v1.1**, and the parts of it that are wrong are precisely the parts the new exam emphasises. This book was written from the v2.0 blueprint itself, topic by topic, in the order Cisco published them.

Who this book is for

- **Network and security engineers** taking the 350-701 SCOR v2.0 exam as the core of a CCNP Security or CCIE Security certification.
- **Engineers moving from routing and switching into security**, who know how a network behaves but have not worked with ISE, Secure Firewall policy, or a cloud security edge.
- **Practising security engineers** who want a structured refresh across the whole domain rather than depth in one product.
- **Anyone who studied the v1.1 material** and needs to know exactly what changed. Appendix A exists for you specifically.

What you are assumed to know

Comfort with IP networking to roughly CCNA level: addressing and subnetting, routing and switching fundamentals, VLANs and trunking, NAT, and the ability to read a device configuration. You do **not** need prior security certification, and every security concept is built from first principles before it is applied.

How the book is organised

Six chapters, one per exam domain, each divided into sub-sections that map **one-to-one onto the numbered blueprint topics**. Sub-section 3.4 in this book is blueprint topic 3.4. Nothing is

merged, nothing is skipped, and nothing is added that the blueprint does not ask for. Page counts are deliberately proportional to the exam weightings, so the time you spend tracks the marks on offer.

Every sub-section follows the same shape: an explanation from first principles, a diagram where the concept is structural, a configuration or worked example, comparison tables where the exam tests “which one, when”, and a closing **Summary** and **Key Takeaways** followed by five exam-style questions with explanations of why each wrong answer is wrong.

The boxes, and what they mean

Box	What it contains
💡 Did you know?	Context and background that makes the concept stick — useful, not examinable in itself
✅ Exam Tip	How the topic is actually tested, and the distinction the question usually turns on
⚠️ Common Pitfall	The mistake people make in the exam or in production, and how to avoid it
🌍 From the Field	How the topic behaves in a real network, from a working engineer's perspective

How to use it

1. **Read a chapter in order.** The sub-sections build on one another and cross-reference forward and backward by number.
2. **Answer the Knowledge Check without looking.** Then read every explanation, including for the questions you answered correctly — the explanations of the wrong options carry as much information as the right one.
3. **Build something.** Appendix C describes a lab you can assemble mostly from free and evaluation software. The Configure topics reward twenty minutes of hands-on far more than an hour of reading.
4. **Use the Key Takeaways as your revision layer.** In the final week they are the fastest route back through the whole book.
5. **Verify the blueprint before you book.** Cisco changes topics without notice; the current version is always on Cisco's certification pages.

The Exam, and How This Book Maps to It

Implementing and Operating Cisco Security Core Technologies v2.0 (350-701 SCOR) is a **120-minute** exam and is the core exam for both **CCNP Security** and **CCIE Security**. The v2.0 blueprint is delivered from **27 August 2026**; the previous v1.1 blueprint was last testable on 26 August 2026.

Domain	Weight	Chapter	Topics	Questions
1.0 Security Concepts	20%	Chapter 1	10	50
2.0 Network Security	25%	Chapter 2	10	50
3.0 Cloud Security	15%	Chapter 3	7	35
4.0 Secure Service Edge	10%	Chapter 4	5	25
5.0 Endpoint Protection and Detection	15%	Chapter 5	7	35
6.0 Network Access, Visibility, and Enforcement	15%	Chapter 6	8	40

Network Security is the largest domain at 25% and carries the most Configure and Troubleshoot verbs, so it deserves the most lab time. **Security Concepts at 20% is the cheapest domain to master**, because almost none of it requires equipment. Together they are 45% of the exam.

Read the verb

Cisco writes each blueprint line with a deliberate verb, and the verb tells you how the topic will be tested.

Verb	How it is tested	How to prepare
Describe / Explain	Scenario and comparison questions — which technology fits this requirement	Reading and comparison tables

Verb	How it is tested	How to prepare
Select	A constraint is given; you choose the model, framework, or deployment	Learn the decision rule for each choice
Configure	The missing command, the wrong command, or the correct order of steps	Learn what depends on what; build it once
Troubleshoot	A symptom is described; you name the cause or the next diagnostic step	Learn the failure signatures, not just the working configuration
Interpret	An artefact is shown — a script, a log, a score, a trajectory — and you say what it means	Practise reading output rather than writing it

What is new in v2.0

If you studied for v1.1, these are the areas where your existing material is silent. Appendix A gives the full topic-by-topic comparison.

- **An entire new domain — 4.0 Secure Service Edge (10%)**, covering SSE and SASE, Cisco Secure Access for both internet and private access, DLP, AI guardrails, and Investigate.
- **AI and LLM vulnerabilities (1.3)** — prompt injection, system prompt leakage, vector and embedding weaknesses, and AI supply chain.
- **Post-quantum cryptography, QUIC, and MASQUE (1.5)**, alongside the classical cryptography topics.
- **Splunk (3.5, 6.6, 6.8)** — ingestion of cloud logging, detection and correlation, and orchestration.
- **Cisco Security Cloud Control (2.4)** as a management option, and **CIS benchmarks (2.5)** for device hardening.
- **Cisco Multicloud Defense and Secure Workload (3.4)**, **eBPF (3.6)**, and **DevSecOps (3.7)**.
- **Cisco XDR (6.6)** and **Duo including Trust Monitor and Continuous Identity Intelligence (6.7)**.

> ✅ **Exam Tip — This book is written for v2.0 only**
>
> Every topic number in this book is a v2.0 topic number. If you are cross-referencing another study resource, check which blueprint it was written for before you trust it — v1.1 material is not merely incomplete for this exam, it spends significant time on content that has been removed.

An Eight-Week Study Plan

This plan assumes roughly eight to ten hours per week and prior CCNA-level networking knowledge. Adjust the pace, not the order: the chapters build on one another. Weight your effort by the exam weighting, which this plan already does.

Week	Reading	Lab and practice
1	Chapter 1, topics 1.1–1.5	Build the lab from Appendix C. Read a TLS handshake in a packet capture
2	Chapter 1, topics 1.6–1.10	Bring up one IPsec tunnel. Read and modify a Python script that calls an API
3	Chapter 2, topics 2.1–2.5	Layer 2 hardening on a switch: port security, DHCP snooping, DAI, BPDU guard
4	Chapter 2, topics 2.6–2.10	FTD access control policy end to end. Break a VPN deliberately and diagnose it
5	Chapter 3, all topics	Ingest one log source into Splunk. Scan an IaC template. Inspect a container
6	Chapter 4, all topics	Walk a Secure Access trial: steering, web policy, private access, Investigate
7	Chapter 5, all topics	Secure Endpoint policy and a trajectory walkthrough on a test detection
8	Chapter 6, then revision	802.1X and MAB with ISE, prove CoA works. Re-read every Key Takeaways block

The final week

1. **Re-answer every Knowledge Check**, marking any question you get wrong or guess.
2. **Re-read only the sub-sections behind your wrong answers** — that is your real syllabus now.

3. **Read all 47 Key Takeaways blocks end to end.** It takes about ninety minutes and is the highest-value revision in the book.
4. **Re-read Appendix A** if you previously studied v1.1, so you do not answer a v2.0 question with v1.1 knowledge.
5. **Skim Appendix B** the morning of the exam — commands and verification steps, nothing new.

> 🌍 **From the Field — On the day**
>
> It is a 120-minute exam and the questions are scenario-shaped, so the failure mode is time rather than knowledge. Read the last sentence of the question first — it tells you what is actually being asked — then read the scenario knowing what you are looking for. Eliminate the two options that contradict something you know for certain before weighing the remaining two. Flag anything that takes more than two minutes and come back to it.

Contents

1.1 The Threat Landscape: On-Premises, Hybrid, and Cloud

A **threat** is an actor or event with the potential to cause harm. A **vulnerability** is a weakness that the threat can use. **Risk** is the intersection of the two, weighted by impact. Keep those three words apart in your head, because the exam mixes them in distractors on purpose: a hard-coded password is a vulnerability, an attacker scanning for it is a threat, and the chance it costs you the customer database is risk.

This sub-section is a taxonomy. Your job is not to memorise malware trivia but to be able to name the class of attack from a two-line description and say which control stops it.

Malware families

Malware is any software written to act against the interests of the system owner. The families overlap, so classify by behaviour:

- **Virus** — attaches to a host file and needs a user to run it. Spreads when the infected file spreads.
- **Worm** — self-propagating; needs no user action. Worms are why flat networks are dangerous: one compromised host reaches every other host on the VLAN.
- **Trojan** — disguises itself as something wanted. The delivery is social, the payload is technical.
- **Rootkit** — hides at or below the operating system (kernel, boot, hypervisor, or firmware level) to make itself and other malware invisible. Because a rootkit subverts the OS itself, tools that ask the OS what is running cannot be trusted — which is why detection moves to boot integrity, memory forensics, and outbound network behaviour.
- **Ransomware** — encrypts data (and increasingly exfiltrates it first for **double extortion**) and demands payment. Modern operations are run as ransomware-as-a-service with affiliates.
- **Fileless malware** — lives in memory and abuses signed system binaries (PowerShell, WMI, `certutil`) — "living off the land." Signature scanning of files finds nothing; behavioural detection does.

> 💡 **Did you know? — Rootkits are ranked by how deep they hide**
>
> A user-mode rootkit hooks API calls inside a process. A kernel-mode rootkit loads as a driver and can lie to every other program. A bootkit infects the bootloader so it loads before the operating system, and a firmware/UEFI implant survives a full disk wipe. Secure Boot and measured boot exist precisely to break the bottom two rungs of that ladder.

Denial of service

A **DoS** attack comes from one source; a **DDoS** attack is orchestrated across many, usually a botnet. Cisco groups them three ways, and the grouping tells you where the mitigation lives:

Category	Examples	Where you mitigate it
Volumetric	UDP/DNS/NTP/memcached amplification, ICMP floods	Upstream — ISP scrubbing or a cloud DDoS service; your own pipe is already full
Protocol / state exhaustion	SYN flood, fragmentation attacks, TCP state table exhaustion	Firewall or load balancer — SYN cookies, embryonic connection limits, rate limits
Application layer	HTTP GET/POST floods, Slowloris, expensive-query abuse	WAF, reverse proxy, application rate limiting and caching

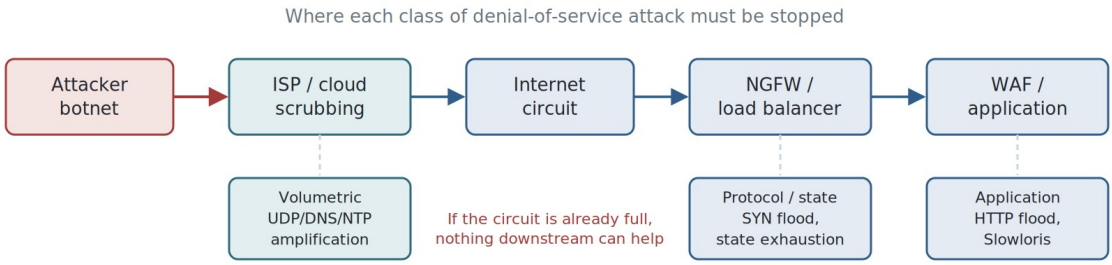

Figure 1.1 — Each class of denial-of-service attack must be stopped at a different point in the path.

> ⚠️ **Common Pitfall — Buying the wrong DDoS control**
>
> A common design error is to buy a bigger firewall to survive a volumetric flood. If the attack saturates your internet circuit, every device behind that circuit is irrelevant — the packets never reach them. **Volumetric defence must be upstream of the bottleneck.** Firewall-based controls answer state-exhaustion and application attacks.

Attacks on identity and the path

- **Phishing** and its variants — spear phishing (targeted), whaling (executives), vishing (voice), smishing (SMS), and quishing (QR codes). Covered in depth in 1.4.
- **Man-in-the-middle / on-path** — the attacker sits in the traffic path and reads or alters it. On a LAN this is ARP spoofing or a rogue DHCP server (defences in 2.3); on the internet it is BGP hijacking, rogue Wi-Fi, or a fraudulent certificate.
- **Compromised credentials** — credential stuffing (reusing breach dumps), password spraying (one common password against many accounts), token or session-cookie theft, and **MFA fatigue** (repeated push prompts until the user approves). Stolen valid credentials are now the most common initial access vector in enterprise breaches, and they defeat every control that assumes "authenticated equals trusted." That single fact is the commercial argument for zero trust in 1.8.
- **Data breach** — the outcome, not the technique: confidential data reaches an unauthorised party, whether by intrusion, an exposed storage bucket, or an insider.

What changes in hybrid and cloud environments

The exam wants you to notice that moving to cloud does not remove threats; it moves them. Three shifts matter:

1. **The control plane becomes internet-facing.** A stolen cloud administrator credential is equivalent to physical access to a data centre. There is no badge reader in front of an API endpoint.
2. **Misconfiguration replaces exploitation.** Public storage buckets, over-permissive IAM roles, and open management ports cause more cloud incidents than software exploits do.

3. **Insecure APIs become the attack surface.** Broken object-level authorisation — changing an ID in a request to read another tenant's record — is the signature cloud API flaw, and it is invisible to a network firewall because the request is perfectly well-formed HTTPS.

> 🌍 **From the Field — The hybrid seam is where incidents start**
>
> In a hybrid estate the weakest point is rarely the on-prem data centre or the cloud provider — it is the connective tissue: the site-to-site VPN with a ten-year-old pre-shared key, the directory-sync service account with domain-admin rights, the jump host that is exempt from posture checks. When you assess a hybrid design, follow the identities that cross the boundary before you look at anything else.

PQC and AI as threat drivers

Two items in this blueprint line are new and are threats rather than technologies:

Post-quantum cryptography (PQC) appears here because of **harvest now, decrypt later**: an adversary records encrypted traffic today and stores it until a cryptographically relevant quantum computer can break the key exchange. Data with a long confidentiality lifetime — health records, state secrets, source code, long-lived certificates — is already at risk even though the quantum computer does not exist yet. The mechanics of the replacement algorithms are in 1.5.

AI raises the quality and volume of attacks: fluent, personalised phishing in any language, voice cloning for vishing, deepfake video used in payment-fraud calls, faster reconnaissance and exploit adaptation, and automated malware variation. It also introduces a brand new attack surface — the models your own organisation deploys — which is what 1.3 covers.

> ✅ **Exam Tip — Two AI questions, two directions**
>
> When a question mentions AI, decide first whether it is about **AI as the attacker's tool** (this sub-section: better phishing, deepfakes, faster recon) or **AI as the target** (1.3: prompt injection, embedding poisoning). The answer options usually contain one of each, and the distinction is the whole question.

Summary

Threats, vulnerabilities, and risk are three different words and the exam tests the difference. Malware classifies by behaviour — viruses need a host and a user, worms self-propagate, trojans lie about what they are, rootkits hide beneath the OS, and fileless malware abuses trusted binaries. DoS attacks split into volumetric, protocol, and application-layer, and each is mitigated at a different point, with volumetric defence necessarily upstream. Identity attacks — phishing, credential stuffing, spraying, token theft, MFA fatigue — now dominate initial access, and hybrid and cloud environments shift risk toward internet-facing control planes, misconfiguration, and insecure APIs. PQC appears as a threat through harvest-now-decrypt-later, and AI appears both as an attacker capability and, in 1.3, as a target.

Key Takeaways

- Threat ≠ vulnerability ≠ risk.
- Worms self-propagate; viruses need a user.
- Rootkits subvert the OS, so trust boot integrity and network behaviour, not the OS's own reports.
- Volumetric DDoS must be scrubbed upstream of your circuit; firewalls handle state and application floods.
- Stolen valid credentials are the leading initial access vector — the core argument for zero trust.
- In cloud, misconfiguration and broken object-level authorisation beat exploitation.
- Harvest now, decrypt later makes PQC a present-day risk for long-lived data.

Knowledge Check — 1.1 The Threat Landscape

Q1. An organisation's internet circuit is saturated by a 40 Gbps DNS amplification flood. Which mitigation will actually restore service?

A. Enabling SYN cookies on the perimeter firewall

B. Adding a WAF in front of the web servers

C. Upstream scrubbing by the ISP or a cloud DDoS provider

D. Lowering the TCP embryonic connection limit on the firewall

Correct answer: C. The attack is volumetric and has already filled the circuit, so every device behind it — firewall, WAF, load balancer — is downstream of the bottleneck and cannot help. SYN cookies and embryonic limits address protocol/state exhaustion; a WAF addresses application-layer floods.

Q2. Malware on a compromised host executes entirely through PowerShell and WMI, leaving no executable on disk. Which description fits best?

A. Fileless malware using living-off-the-land techniques

B. A boot-sector virus

C. A network worm

D. A user-mode rootkit

Correct answer: A. Abusing signed, built-in system binaries with a memory-resident payload is the definition of fileless, living-off-the-land malware. It is not a virus (no infected host file), not a worm (no self-propagation described), and not a rootkit (nothing is described as hiding the OS's own view of itself).

Q3. Which statement best captures why 'harvest now, decrypt later' makes post-quantum cryptography an issue today?

A. Quantum computers can already break AES-256 in production

B. TLS 1.3 removed forward secrecy, leaving sessions replayable

C. Existing certificates expire faster than PQC certificates would

D. Captured ciphertext can be stored now and decrypted once quantum capability arrives, so long-lived secrets are already exposed

Correct answer: D. The risk is temporal: today's recorded traffic is tomorrow's plaintext if the key exchange is quantum-vulnerable, which matters for data with a long confidentiality lifetime. No quantum computer breaks AES-256 in production, TLS 1.3 mandates forward secrecy rather than removing it, and certificate lifetime is unrelated.

Q4. An attacker tries the single password 'Autumn2026!' against 4,000 user accounts, one attempt per account. What is this?

A. Credential stuffing

B. Password spraying

C. A brute-force attack against one account

D. An MFA fatigue attack

Correct answer: B. Spraying uses one or a few likely passwords across many accounts specifically to stay under per-account lockout thresholds. Credential stuffing replays username/password pairs from previous breaches; brute force hammers a single account; MFA fatigue floods a user with push approvals.

Q5. Which risk is most characteristic of insecure cloud APIs rather than traditional network attacks?

A. ARP cache poisoning between hosts in the same VLAN

B. A SYN flood exhausting the firewall connection table

C. VLAN hopping using double-tagged frames

D. Broken object-level authorisation, where changing an identifier in a valid request returns another tenant's data

Correct answer: D. Broken object-level authorisation is an application-logic flaw: the request is well-formed, authenticated HTTPS, so network controls see nothing wrong. The other three are Layer 2 or transport attacks addressed by switch hardening and stateful inspection.

End of sample

The full guide continues for another 330 pages.

- 6 chapters, one per exam domain
- 47 sub-sections mapped to the v2.0 blueprint
- 235 exam-style questions, every option explained
- 34 original diagrams and worked configurations
- What changed from v1.1 to v2.0
- Command reference, practice lab, and glossary

Get the complete guide

leanpub.com/scor

SCOR 350-701 · Complete Learning Guide · Exam version v2.0

Independent · Unofficial Study Guide

No exam content. Ever.