CCNP Security, Blueprint Updates

Blueprint Revisions

Products and technologies are evolving faster than ever before. To ensure that our certification programs remain relevant to current practice and keep up with the fast pace of change, we are committed to an annual maintenance review. Minor reviews ensure exam topics are clear, introduce new topics, and phase out older products and solutions that are less relevant today. The aim is to make the minor adjustments needed to match the evolution of technologies while ensuring the changes are minimal so that they do not disrupt a candidate's study plans.

The CCNP Security exam portfolio just completed an update to keep the domains closely aligned with today's commonly adopted technologies and solutions. Below is a summary of the blueprint changes that will go live on August 27, 2026.

350-701 Implementing and Operating Cisco Security Core Technologies		
v1.1 to v2.0		
20%	**1.0**	**Security Concepts**
	1.1	Explain attack threats against on-premises, hybrid, and cloud environments such as viruses, trojans, DoS/DDoS, phishing, rootkits, man-in-the middle, malware, data breaches, insecure APIs, compromised credentials, PQC, and AI
	1.2	Describe security vulnerabilities and exploits such as software bugs, weak and/or hardcoded passwords, OWASP top ten, missing encryption ciphers, buffer overflow, path traversal, cross-site scripting/forgery, SQL injection, and identification and prioritization using CVEs and CVSS scores
	1.3	Describe vulnerabilities in AI/LLM models such as prompt injection, system prompt leakage, vector and embedding weaknesses, and supply chain
	1.4	Describe the controls used to protect against phishing and social engineering attacks
	1.5	Describe cryptography security components such as hashing, encryption, PKI, SSL, TLS, QUIC, MASQUE, IPsec, NAT-T IPv4 for IPsec, preshared key, certificate-based authorization, and post-quantum cryptography
	1.6	Describe site-to-site and remote access VPN deployment types such as virtual tunnel interfaces, standards-based IPsec, SSL VPN, DMVPN, FlexVPN, and GETVPN
	1.7	Describe security intelligence authoring, sharing, and consumption
	1.8	Describe zero trust architecture
	1.9	Describe defense in depth strategy such as Secure Architecture for Everyone (SAFE)
	1.10	Interpret scripts used to call security appliances APIs in a language such as Python
25%	**2.0**	**Network Security**
	2.1	Describe network security solutions and deployment models that provide intrusion prevention and firewall capabilities
	2.2	Describe security monitoring and telemetry technologies
	2.3	Configure network infrastructure security methods (network segmentation using VLANs or SGTs; Layer 2 and port security; DHCP snooping; Dynamic ARP inspection; storm control; and defenses against MAC, ARP, VLAN hopping, STP, and DHCP rogue attacks)
	2.4	Select management options for network security solutions (single vs. multidevice manager, in-band vs. out-of-band, on-premises vs. cloud with Cisco Security Cloud Control)
	2.5	Describe CIS benchmarks for hardening devices such as Cisco Secure Firewall (FTD) and Cisco IOS XE
	2.6	Troubleshoot AAA for device and network access such as TACACS+ and RADIUS

Cisco and Cisco logo are trademarks or registered of Cisco and/or its affiliates in the U.S. and other countries.
To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.
Cisco © and/or its affiliates. All rights reserved.

CCNP Security, Blueprint Updates

	2.7	Configure secure network management of perimeter security and infrastructure devices such as SNMPv3, NetConf, RestConf, APIs, secure syslog, and NTP with authentication
	2.8	Implement access control policies, AVC, URL filtering, malware protection, and intrusion prevention using Cisco Secure Firewall (FTD)
	2.9	Configure site-to-site and remote access VPN using Cisco Secure Firewall (FTD) and Cisco Secure Client
	2.10	Troubleshoot VPN tunnel establishment on Cisco Secure Firewall (FTD)
15%	**3.0**	**Cloud Security**
	3.1	Describe security responsibility within common Cloud Shared Responsibility Models
	3.2	Select security capabilities, deployment models, cloud security frameworks, and policy management to secure the cloud
	3.3	Select security solutions for cloud environments (public; private; hybrid; community cloud; NIST 800-145 SaaS, PaaS, and IaaS; and Cloud Access Security Broker)
	3.4	Describe network, application, and data security in cloud environments with solutions such as Cisco Multicloud Defense and Cisco Secure Workload
	3.5	Configure Splunk to ingest cloud logging and monitoring data from other security solutions
	3.6	Describe application and workload security concepts including eBPF
	3.7	Describe DevSecOps (Infrastructure as Code security, CI/CD pipeline, container orchestration, and secure software development)
10%	**4.0**	**Secure Service Edge**
	4.1	Describe Security Service Edge (SSE) and Secure Access Service Edge (SASE)
	4.2	Configure Cisco Secure Access Secure Internet Access
	4.3	Configure Cisco Secure Access Secure Private Access
	4.4	Configure data loss prevention and AI guardrails for secure internet access
	4.5	Interpret Cisco Secure Access Investigate scores and indicators
15%	**5.0**	**Endpoint Protection and Detection**
	5.1	Describe Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR) solutions
	5.2	Describe endpoint device management and asset inventory systems such as MDM
	5.3	Describe endpoint posture assessment solutions to ensure endpoint security
	5.4	Describe endpoint protection and detection security with solutions such as Cisco Secure Client and Cisco Secure Malware Analytics
	5.5	Configure endpoint antimalware protection using Cisco Secure Endpoint
	5.6	Interpret Cisco Secure Endpoint malware detection events
	5.7	Configure email security features with Cisco Security Email Threat Defense
15%	**6.0**	**Network Access, Visibility, and Enforcement**
	6.1	Describe identity management and secure network access concepts such as guest services, profiling, posture assessment, and BYOD
	6.2	Describe device compliance and application control
	6.3	Configure network access control mechanisms such as 802.1X and MAB with Cisco Identity Services Engine
	6.4	Configure network access with CoA
	6.5	Explain exfiltration techniques such as DNS tunneling, HTTPS, email, FTP/SSH/SCP/SFTP, ICMP, Messenger, IRC, NTP, and cloud storage
	6.6	Describe network visibility and enforcement using telemetry and native AI/ML capabilities with XDR and SIEM/SOAR platforms such as Splunk and Cisco XDR
	6.7	Describe Cisco Duo in a zero-trust security architecture (Trust Monitor, MFA, Device Trust, health checks, Adaptive Access policies, SSO, and CII)
	6.8	Describe managing, orchestrating and automating security information and events with Splunk

Cisco and Cisco logo are trademarks or registered of Cisco and/or its affiliates in the U.S. and other countries.
To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.
Cisco © and/or its affiliates. All rights reserved.

CCNP Security, Blueprint Updates

300-710 Securing Networks with Cisco Firewalls

v1.1 to v1.2

2.2 Configure security policies such as access control, DNS, identity, and network analysis policy in Secure Firewall Management Center
- 2.2.a ~~Access control~~
- 2.2.b ~~Intrusion~~
- 2.2.c ~~Malware & File~~
- 2.2.d ~~DNS~~
- 2.2.e ~~Identity~~
- 2.2.f ~~Decryption~~
- 2.2.g ~~Prefilter~~

2.5 Configure devices using Secure Firewall Management Center
- 2.5.a Device management such as certificates, platform setting, and health policy
- 2.5.b Network settings such NAT, QoS, and routing
- 2.5.c Secure access such as zero trust network access and VPN
- 2.5.a ~~Device management~~
- 2.5.b ~~NAT~~
- 2.5.c ~~VPN~~
- 2.5.d ~~QoS~~
- 2.5.e ~~Platform settings~~
- 2.5.f ~~Certificates~~
- 2.5.g ~~Routing~~

3.3 Troubleshoot Firewall Threat Defense using tools:
- 3.3.a Packet capture procedures
- 3.3.b Packet Tracer
- 3.3.c Firewall engine debug
- 3.3.d System Support Trace

3.4 Analyze risk and standard reports such as events (connection, discovery, intrusion, malware, and unified) and network map

3.5 Describe device management tools
- 3.5.a ~~Cisco Defense Orchestrator~~
- 3.5.b Cisco Security Cloud Control Firewall Management (formerly Cloud-delivered Firewall Management Center)
- 3.5.c Secure Firewall Device Manager
- 3.5.d Secure Firewall Management Center

4.8 Describe Splunk integration and AI-driven threat intelligence

300-715 Implementing and Configuring Cisco Identify Services Engine

v1.1 to v1.2

2.2 Describe identity store options
- 2.2.a LDAP
- 2.2.b AD
- 2.2.c PKI
- 2.2.d Multifactor authentication

Cisco and Cisco logo are trademarks or registered of Cisco and/or its affiliates in the U.S. and other countries.
To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.
Cisco © and/or its affiliates. All rights reserved.

CCNP Security, Blueprint Updates

	2.2.e	Local
	2.2.f	~~SAML IDP~~
	2.2.g	~~Rest ID~~
2.4	Configured wired network access using 802.1x and IBNS 2.0	
	2.4.a	Monitor mode
	2.4.b	Low impact
	2.4.c	Closed mode
	2.4.d	Host mode
5.4	~~Configure block list/allow list~~	
5.4	Implement BYOD device lifecycle operations	
6.3	~~Configure the compliance module~~	
6.4	Configure posture ~~agents and operational modes~~ services with the Cisco ISE Posture Work Center	
6.5	~~Describe supplicant, supplicant options, authenticator, and server~~	

This exam has major blueprint changes coming end of March 2026

- 300-740 Designing and Implementing Secure Cloud Access for Users and Endpoints

This exams have no blueprint changes

- 300-745 Designing Cisco Security Infrastructure

These exams will end of life on August 27, 2026

- 300-720 Securing Email with Cisco Secure Email Gateway
- 300-725 Securing the Web with Cisco Secure Web Appliance
- 300-730 Implementing Secure Solutions with Virtual Private Networks

Cisco and Cisco logo are trademarks or registered of Cisco and/or its affiliates in the U.S. and other countries.
To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.
Cisco © and/or its affiliates. All rights reserved.