Cisco 500-285 Exam Prep: Security Architecture

Cisco 500-285 2026. Security architecture, appliance configuration, threat analysis, and security policies.

IT Certifications Instructor: Brian Mitchell • 5 sections • 46 lessons • 15.25h total

View this course online Browse all courses

About this course

Preparing for the Cisco 500-285 exam can feel overwhelming with the breadth of security technologies involved. This course breaks down the key exam objectives into manageable, real scenarios. We focus on the practical application of Cisco security solutions, moving beyond just definitions to understand how these tools work together in a live environment.

You will get a step-by-step guide to configuring essential security appliances, analyzing threat data, and applying security policies. The course includes video walkthroughs of key configurations, downloadable cheat sheets for exam topics, and practical case studies based on common network security challenges.

Course curriculum

Foundations and Preparation

- Understanding the 500-285 Exam Blueprint (12m)
  We'll break down the official exam topics to show you exactly what Cisco expects, helping you prioritize your study time effectively.
- Core Security Principles and Terminology (18m)
  Learn the fundamental security concepts and Cisco-specific terms you'll encounter on the exam and in the field.
- Navigating Cisco Security Product Families (15m)
  A clear overview of the Cisco Secure portfolio, including Firepower, Umbrella, and SecureX, so you know which tool does what.
- Setting Up Your Study Lab Environment (25m)
  A practical guide to setting up a virtual lab using Cisco modeling tools to practice configurations safely.
- Key Network Protocols for Security Professionals (22m)
  Review essential protocols like TLS, DNS, and IPsec, focusing on their security implications and role in Cisco solutions.
- Introduction to Security Deployment Models (16m)
  We'll explain cloud, on-premise, and hybrid security models, and how Cisco solutions fit into each architecture.
- Creating Your Personal Study Plan (8m)
  A step-by-step guide to building a realistic study schedule that covers all exam domains before your test date.
- Common Exam Pitfalls and How to Avoid Them (14m)
  Learn about common mistakes test-takers make and get practical advice on how to approach tricky exam questions.

Core Security Solutions

- How Cisco Firepower NGFW Works (28m)
  A deep dive into the architecture of Next-Generation Firewalls, explaining how it inspects traffic to stop threats.
- Configuring Basic Access Control Policies (22m)
  A hands-on walkthrough of creating and applying access control rules to permit or block traffic effectively.
- Understanding Cisco Umbrella and DNS Security (19m)
  Learn how Umbrella provides a first line of defense by blocking malicious domains before a connection is even established.
- Deploying the Cisco Secure IPS Module (31m)
  We'll show you how to configure and tune the Intrusion Prevention System to detect and block known exploits.

- Introduction to Cisco Secure Endpoint (AMP) (17m)
  Explore how Advanced Malware Protection analyzes file behavior to detect and block malware on endpoints.
- Working with Security Intelligence Feeds (15m)
  Learn how to subscribe to and apply threat intelligence feeds to keep your defenses up-to-date with the latest threats.
- Basics of Cisco Secure Email Gateway (20m)
  Understand how to configure basic policies to filter spam, block phishing attempts, and scan email attachments.
- Introduction to Cisco Secure Web Appliance (18m)
  Learn the fundamentals of web filtering and URL categorization to protect users from malicious websites.
- Using Dashboards for Security Monitoring (12m)
  A practical look at Cisco's security dashboards to help you quickly identify and respond to security events.

Advanced Threat Detection

- Deep Packet Inspection and File Trajectory (26m)
  We'll explore how Firepower tracks a malicious file across your network to identify all impacted hosts.
- Tuning Intrusion Policies for Performance (24m)
  Learn how to balance security and performance by fine-tuning your intrusion rules and preprocessor settings.
- Analyzing Security Events and Alerts (21m)
  A real case study analysis of security event data to separate false positives from genuine threats.
- Implementing Network Address Translation (NAT) (19m)
  A step-by-step guide to configuring NAT policies within the Firepower Management Center for secure traffic.
- Understanding Site-to-Site VPNs with Cisco (32m)
  We'll configure a basic IPsec VPN tunnel between two sites to understand secure data transmission.
- Remote Access VPN Solutions Overview (18m)
  Explore Cisco's remote access VPN options, including AnyConnect, and their key security features.
- Using Cisco SecureX for Threat Response (23m)
  Learn how to automate your response to threats by orchestrating actions across different Cisco security products.

Policy and Management

- Building a Scalable Security Architecture (25m)
  Learn how to design a security policy framework that can grow with your organization's needs.
- User and Identity-Based Policies (29m)
  A practical guide to integrating identity sources like Active Directory to create user-specific security rules.
- Configuring SSL Decryption Policies (27m)
  We'll show you how to inspect encrypted traffic to find hidden threats without compromising privacy.

- Managing User Access and Admin Roles (15m)
  Learn how to set up role-based access control in the FMC to ensure admins only have the permissions they need.
- Backup and Restore for Security Appliances (14m)
  A crucial lesson on creating and managing backups of your security policies and configurations.
- Troubleshooting Common Connectivity Issues (33m)
  A problem-solving session focused on diagnosing and fixing common traffic flow and policy misconfiguration errors.
- Compliance Reporting and Auditing (16m)
  Learn how to generate reports that demonstrate compliance with standards like PCI-DSS and HIPAA.
- Automating Tasks with REST APIs (28m)
  An introduction to using basic API calls to pull data and automate simple tasks in your security environment.
- Best Practices for System Health Monitoring (13m)
  Get a checklist for monitoring the health and performance of your Cisco security appliances.
- Updating and Patching Your Security Devices (11m)
  A straightforward guide to managing software updates and patches to keep your defenses secure.

Implementation & Next Steps

- Full Lab: Deploying a Multi-Layer Security Policy (38m)
  A capstone project where you'll build a complete security policy from the ground up, integrating multiple products.
- Scenario: Responding to a Ransomware Outbreak (25m)
  We'll walk through the steps of isolating, analyzing, and remediating a simulated ransomware attack.
- Scenario: Investigating a Data Exfiltration Attempt (22m)
  Learn how to use your security tools to trace the path of stolen data and identify the source of the breach.
- Scenario: Mitigating a DDoS Attack (20m)
  A practical look at how to use Cisco solutions to identify and mitigate the impact of a Distributed Denial of Service attack.
- Scenario: Dealing with a Phishing Campaign (17m)
  Learn how to use email security and endpoint protection tools to block a widespread phishing campaign.
- Final Exam Review: Key Concepts and Commands (30m)
  A comprehensive review of the most critical topics, configurations, and concepts you need to remember for the exam.
- Practice Exam Strategy and Question Walkthrough (28m)
  We'll analyze sample exam questions and discuss strategies for selecting the correct answer under pressure.
- Career Paths After Your Cisco Security Cert (12m)
  Explore potential job roles and how to leverage your new certification to advance your career in cybersecurity.

- Downloadable Resources and Template Library (5m)
  Get access to a collection of downloadable templates, checklists, and cheat sheets to use on the job.
- Staying Current: Continuous Learning in Security (9m)
  Discover the best blogs, communities, and resources to stay up-to-date in the fast-changing world of cybersecurity.
- Your 30-Day Post-Exam Action Plan (10m)
  A clear plan for what to do immediately after passing your exam to start applying your skills in the real world.
- Course Wrap-Up and Final Encouragement (6m)
  A brief conclusion to summarize your journey, celebrate your hard work, and wish you luck on exam day.

Discover our blog

Learn more with free articles written by our professors and guest experts.

Latest article: **Flight Attendant Preparation: What to Study Before You Apply**

Visit the blog All courses This course