Cisco 500-470: Enterprise Network Security Design

Prepare for Cisco 500-470 with practical enterprise network security design strategies.

IT Certifications Instructor: Jason Miller • 5 sections • 46 lessons • 18.50h total

View this course online Browse all courses

About this course

This course helps you prepare for the Cisco 500-470 exam, focusing on real-world enterprise network security design. We cover the core principles of securing networks, from foundational concepts to threat mitigation strategies, using practical examples that mirror what you will face in professional environments.

You will learn how to design secure network architectures, implement security controls, and apply practices for protecting enterprise infrastructure. Through step-by-step guides, real case study analysis, and problem-solving sessions, you will gain the hands-on skills needed to pass the exam and apply these concepts in your work.

Course curriculum

Foundations and Preparation

- Understanding the 500-470 Exam Structure (12m)
  Break down the exam blueprint and understand what topics are weighted most heavily for success.
- Core Network Security Principles (18m)
  Learn the foundational security concepts that form the basis of all enterprise network design decisions.
- Cisco Security Portfolio Overview (15m)
  Get familiar with key Cisco security products and their roles in modern enterprise networks.
- Threat Landscape for Enterprise Networks (22m)
  Analyze common attack vectors and understand what you're protecting against in real scenarios.
- Security Design Methodology (16m)
  Step-by-step guide to the Cisco security design framework and approach.
- Compliance and Regulatory Considerations (20m)
  Understand how compliance requirements shape security design decisions in regulated industries.
- Building Your Study Plan (8m)
  Create a practical study schedule that fits your timeline and learning style.

Core Security Architecture Concepts

- Designing Secure Network Topologies (28m)
  Learn how to structure networks with security as the primary design consideration.
- Segmentation Strategies with Cisco (25m)
  Implement microsegmentation and network segmentation using Cisco security tools.
- Identity and Access Management Design (30m)
  Design robust IAM solutions that balance security with user experience.
- Cisco Firepower Threat Defense Architecture (26m)
  Deep dive into FTD deployment options and design considerations.
- Secure Remote Access Design (24m)
  Design VPN and remote access solutions that meet enterprise security requirements.
- Wireless Security Design Principles (22m)
  Secure wireless networks with proper authentication and encryption strategies.
- Email Security Architecture (19m)
  Design email security solutions to protect against phishing and malware threats.
- Web Security and Content Filtering (21m)
  Implement web security controls to prevent malware delivery and data exfiltration.
- Endpoint Security Integration (27m)
  Integrate endpoint protection into your overall security architecture design.

Advanced Security Technologies

- Cisco Umbrella DNS Security (31m)
  Deploy and design DNS-layer security using Cisco Umbrella for threat prevention.
- Stealthwatch for Network Visibility (29m)
  Use Stealthwatch to design comprehensive network monitoring and threat detection.
- Cisco ISE for Policy Enforcement (33m)
  Design network access control policies using Cisco Identity Services Engine.
- Advanced Malware Protection Design (23m)
  Implement AMP for endpoints and networks to detect and block advanced threats.
- Security Group Tagging and SGT (20m)
  Design scalable security policies using Cisco's Security Group Tagging.
- Encrypted Traffic Analytics (26m)
  Design security monitoring for encrypted traffic without decrypting everything.
- Cloud Security with Cisco (28m)
  Extend security architecture into cloud environments using Cisco solutions.
- Zero Trust Architecture Design (35m)
  Apply zero trust principles to enterprise network security design.

Implementation and Integration

- Multi-Vendor Security Integration (24m)
  Design solutions that integrate Cisco security with third-party tools and systems.
- High Availability Security Design (32m)
  Build resilient security architectures with redundancy and failover capabilities.
- Performance Tuning for Security Appliances (26m)
  Optimize security device performance while maintaining protection levels.
- Scalability Considerations (28m)
  Design security solutions that scale with organizational growth.
- Automation for Security Deployment (30m)
  Use automation tools to deploy and manage security configurations at scale.
- Monitoring and Alerting Design (27m)
  Design comprehensive monitoring and alerting for security operations.
- Incident Response Integration (25m)
  Design security architecture to support rapid incident detection and response.
- Logging and Reporting Design (22m)
  Design logging infrastructure that meets compliance and operational needs.
- Change Management for Security (18m)
  Design processes for safely implementing security changes in production.
- Capacity Planning for Security Infrastructure (21m)
  Plan for current and future security infrastructure requirements.

Real-World Application and Exam Strategy

- Case Study: Financial Services Security Design (35m)
  Real case study analysis of a complex financial services security implementation.
- Case Study: Healthcare Network Security (38m)
  Analyze security design challenges in HIPAA-regulated healthcare environments.
- Case Study: Manufacturing OT/IT Convergence (34m)
  Design security for industrial networks with operational technology requirements.
- Case Study: Retail Multi-Site Security (32m)
  Design scalable security for distributed retail environments.
- Common Design Mistakes to Avoid (20m)
  Learn from real failures and how to avoid them in your designs.
- Exam Question Strategies (25m)
  Approach 500-470 exam questions with confidence using proven strategies.
- Time Management During the Exam (15m)
  Techniques for pacing yourself and completing all questions effectively.
- Troubleshooting Design Scenarios (29m)
  Problem-solving session on common design issues and their solutions.
- Documentation and Diagramming Best Practices (18m)
  Create clear, professional security design documentation for stakeholders.
- Stakeholder Communication for Security Designs (16m)
  Present security designs to technical and non-technical audiences effectively.
- Final Review and Key Concepts (28m)
  Comprehensive review of all critical exam topics and design principles.
- Next Steps After Certification (12m)
  Plan your career development and continuing education in Cisco security.