

CompTIA Sec+ SY0-501, Part 4 of 9: Network Design and Cloud

page 1

Meet the expert: Jason Dion, CISSP No. 349867, is a professor at University of Maryland University College with multiple information technology professional certifications, including Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Network Defense Architect (CNDA), Digital Forensic Examiner (DFE), Digital Media Collector (DMC), CySA+, Security+, Network+, A+, PRINCE2 Practitioner, and ITIL. He holds a Masters of Science degree in Information Technology with a specialization in Information Assurance

Prerequisites: • Basic familiarity with computer networks, administration, and security is helpful (But, all required information will be covered during the course)
• Completion of the CompTIA A+ and Network+ certifications (Helpful, but not required)

Runtime: 01:18:17

Course description: This course discusses network design with the OSI model, switchers, routers as well as access, sub-netting and telephony. Next, it discusses perimeter security, as well as proxy servers, honeypots and unified threat management. Finally, it covers Cloud Security for the SY0-501 Exam.

Course outline:

Network Design

- Introduction
- Network Security
- OSI Model
- Switches
- Routers
- Network Zones
- Summary
- Cloud Computing
- Cloud Types
- As a Service
- Cloud Security
- Defending Servers
- Summary

Network Access

- Introduction
- Network Access Control (NAC)
- VLANs
- Subnetting
- Network Address Translation
- Telephony Devices
- Summary

Perimeter Security

- Introduction
- Perimeter Security
- Firewalls
- Demo: SOHO Firewall
- Proxy Servers
- Honeypots and Honeynets
- Data Loss Prevention
- NIDS vs NIPS
- Unified Threat Management
- Summary

Cloud Security

- Introduction