CCNP Security - SISAS
Implementing Cisco Secure Access Solutions

Instructor Introduction

- Cristian Matei, CCIE #23684
  - CCIE Security – 2009
  - CCIE Routing and Switching – 2011
- Contact
  - cmatei@ine.com
  - @christianmatei
  - ro.linkedin.com/in/christianmatei

Live Online Classroom Overview

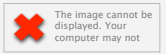
- Adjusting your bandwidth
  - HD button on bottom right of player adjusts stream
- Using the Q&A session
  - All questions are submitted to me privately
  - Questions relevant to everyone will be posted publicly
- Course Files
  - Slides, diagrams, etc. posted in link above Q&A session
- Course is recorded
  - Recordings will be available in Course Library after post-processing

Course Schedule

- Course length is 4 days
- Daily schedule
  - Starts at 07:00 AM PDT
  - Runs about 4-8 hours
  - Breaks
    - ~ 10 minutes hourly
    - ~ 30 minutes at half

Course Format

- Course is a mix of…
  - Technology discussion
  - Hands-on examples with troubleshooting
- Technology Discussion
  - Slides, whiteboards, online references
- Hands-on examples
  - Live examples on real equipment
  - Not pre-tested, so troubleshooting may be required



Course Pre-Requisites

Technical Knowledge

- Basic knowledge of networking technologies
  - Ideally CCNA R&S certified or equivalent knowledge
  - E.g. what is OSI, TCP/IP, Ethernet, etc.
  - E.g. what are switches, routers, servers, etc.
- Basic knowledge of security technologies
  - Ideally CCNA Security certified or equivalent knowledge
- Working knowledge of Cisco IOS and ASA operating system
- Working knowledge of Windows operating system

Course Intended Audience

- CCNP Security Certification candidates
  - Obviously ☺
- Everyday entry/intermediate level engineers
  - Getting your feet wet in the world of security, apply knowledge in real-world implementations
- Class focus is understanding technologies
  - For CCNP Security candidates, get certified as a byproduct of understanding the technologies

Course Scope

- What is the scope of this class?
  - Provide a structured learning methodology
    - Move away from the command memorization concept
    - Learn technologies, not commands
    - To gain knowledge there is no shortcut
  - Understand the technologies relevant to the blueprint
  - Help you pass the exam for getting certified
    - There is no one single resource (book, video series) that can get you certified

What is CCNP Security?

- Cisco's Intermediate-level certification on Security track
- Cisco's Description
  - *"Cisco Certified Network Professional Security (CCNP Security) certification program is aligned specifically to the job role of the Cisco Network Security Engineer responsible for Security in Routers, Switches, Networking devices and appliances, as well as choosing, deploying, supporting and troubleshooting Firewalls, VPNS, and IDS/IPS solutions for their networking environments."*

What is SISAS?

- Cisco's Identity Services Engine
- Cisco's Description
  - *"The Implementing Cisco Secure Access Solutions (SISAS) (300-208) exam tests whether a network security engineer knows the components and architecture of secure access, by utilizing 802.1X and Cisco TrustSec. This 90-minute exam consists of 65-75 questions and assesses knowledge of Cisco Identity Services Engine (ISE) architecture, solution, and components as an overall network threat mitigation and endpoint control solutions. It also includes the fundamental concepts of bring your own device (BYOD) using posture and profiling services of ISE. Candidates can prepare for this exam by taking the Implementing Cisco Secure Access Solutions (SISAS) course."*

Course Description

- Course is based on SISAS v1.0 Blueprint
  - Implementing Cisco Secure Access Solutions (300-208)
  - More specifics at http://www.cisco.com/go/ccnpsecurity
- Course Outline
  - AAA and ISE Concepts
  - Authentication and Authorization
  - Secure Access Deployment Modes
  - Web Services
  - Profiling and Posture
  - Trustsec

Course Outline

- AAA and ISE Concepts
  - AAA Terminology
  - RADIUS vs. TACACS
  - ISE Fundamentals
- Authentication
  - MAB
  - EAPOL Framework (802.1x)
  - EAP-FAST, PEAP, EAP-MSCHAPv2, EAP-TLS, EAP Chaining
  - Active Directory Integration
  - Troubleshooting

Course Outline

- Authorization
  - ACL
  - VLAN
  - Troubleshooting
- Secure Access Deployment Modes
  - Monitor Mode
  - Low Impact Mode
  - Closed Mode
  - Troubleshooting

Course Outline

- Web Services
  - Central Web Authentication
  - RADIUS Change of Authorization (RFC 3576)
  - Guest Services
  - Bring Your Own Device
  - Troubleshooting
- Profiling and Posture
  - Profiling Sources
  - NAC Agent Client Provisioning and Posture Assessment
  - Troubleshooting

Course Outline

- TrustSec
  - MacSec (802.1ae)
  - Security Group Tags (SGT)
  - Security Group Exchange Protocol (SXP)
  - Troubleshooting

Q&A