Cisco CCNA Security

Cisco CCNA Security cursus - Overview

- Training schedule :
  - 12 Thursdays
  - From January 25th to May 3rd
  - From 18h15 To 21h15
- Training objective :
  - Understand core security concepts and develop skills in implementing security policies to mitigate risks
  - Prepare to the Cisco CCNA Security certification exam

Cisco CCNA Security cursus - Note

- *Les cours se donnent en français*
- Supports are in English & French

Cisco CCNA Security cursus - Instructor

- Instructor: Laurent SCHALKWIJK
  - CCNP (certificate verification N°: 402324168200BQUN)
  - ASA Specialist (certificate verification N°: 417494173250ATXF)
  - CCNA Voice (certificate verification N°:410634172094BMCI)
  - CCNA Wireless (certificate verification N°:410564171733EOAM)
  - CCNA Security (certificate verification N°: 410354170858EMXH)
  - CCNA (certificate verification N°: 391034725042ELXF)
  - Qualified Instructor CCNA (CCAI) et ITQ (Instructor teacher)

Cisco CCNA Security cursus - Program

- Features :

- **Eleven modules** of interactive instructional content
- **Activities**, including Packet Tracer activities
- Assessments include module quizzes, **practice exams and final exam**
- Estimated time to complete: **70 hours** / full semester course
- **Certificate** of Completion and CEO Letter
- **Prerequisites** for certification : **CCENT-level** networking knowledge and skills
- This course prepares to certification but certification process must be done in Pearson Vue Center

Cisco CCNA Security cursus - Target audience

- Target audience :
  - **IT professionals** wishing to broaden skills or add specialized technology expertise
  - Current Cisco CCENT or CCNA Certification holders who wish to build CCNA knowledge

Cisco CCNA Security cursus - Planning

- Cursus sequence :
  - 18h15 - 19h30 : Training,
  - 19h30 - 19h45 : Break,
  - 19h45 - 21h15 : Training.

Cisco CCNA Security cursus - Key competencies

Upon completion of this course, students will be able to:

- Describe **security threats** facing modern network infrastructures
- **Secure** Cisco **routers** and **switches**
- Describe **AAA functionalities** and implement AAA on Cisco routers using local router database and server-based ACS or ISE
- Mitigate threats to networks using **ACLs and stateful firewalls**
- Implement **IPS** and **IDS** to secure networks against evolving attacks
- Mitigate threats to email, web based and endpoints attacks and **common Layer 2 attacks**
- Secure communications to ensure **integrity**, **authenticity** and **confidentiality**.

Cisco CCNA Security cursus - Key competencies

- Describe the purpose of **VPNs**, and implement Remote Access and Site-to-Site VPNS.
- Secure networks using **ASA**