

Cisco 210-260 IINS Implementing Cisco Network Security

Cisco CCNA Security

210-260 IINS Implementing Cisco Network Security 3.0



3a Kypca

- In this course, you will learn about the design, implementation, and monitoring of a comprehensive security policy using Cisco IOS security features and technologies as examples. You will also learn about security controls of Cisco IOS devices as well as a functional introduction to the Cisco Adaptive Security Appliance (ASA). This course enables you to perform basic tasks to secure a network using Cisco IOS security features, which are available through web-based GUIs on the Cisco ASA, and the command-line interface (CLI) on Cisco routers and switches. Site-to-site virtual private network (VPN) configuration is covered on both the Cisco IOS and the Cisco ASA. Modern malware examples are included in this course as are cryptographic techniques using stronger hashing and encryption algorithms.

Current versions of Cisco IOS, Cisco ASA, and Cisco AnyConnect are featured.

Цели – Какво ще научите

- Common network security concepts
- Secure routing and switching infrastructure
- Deploy basic authentication, authorization, and accounting services
- Deploy basic firewalling services
- Deploy basic site-to-site and remote access VPN services
- Advanced security services such as intrusion protection, content security and identity management
- Develop a comprehensive network security policy to counter threats against information security
- Configure routers with Cisco IOS software security features, including management and reporting functions
- Bootstrap the Cisco ASA Firewall for use in a production network
- Configure the Cisco ASA Firewall for remote access to a Secure Sockets Layer (SSL) VPN
- Configure a Cisco IOS zone-based firewall (ZBF) to perform basic security operations on a network
- Configure site-to-site VPNs using Cisco IOS features
- Configure security features on IOS switches to mitigate various Layer 2 and Layer 3 attacks
- How a network can be compromised using freely available tools
- Implement line passwords, and enable passwords and secrets
- Examine authentication, authorization, and accounting (AAA) concepts and features using the local database as well as Cisco Secure ACS 5.2
- Configure packet filtering on the perimeter router

Курсът е предназначен за

- Network designers
 - Network, systems, and security engineers
 - Network and security managers
-

Формат на курса



Присъствен Курс



**Онлайн (Live)
Отдалечен**

Език на курса: български (английски е наличен като опция)

Учебни Материали: в електронен формат (Учебните материали са на английски), включени в цената с неограничен достъп.

Лабораторна среда: всеки курсист разполага със собствена лаб среда, където се провеждат упражненията, част от курса.

Продължителност

- 5 работни дни (понеделник – петък 09:00 – 17:00)

или

- **40 уч.ч. обучение (теория и практика) в извънработно време с продължителност 1 седмици**
 - събота и неделя 10:00 – 14:00, 14:00 – 18:00, 18:00 – 22:00
 - понеделник и сряда 19:00 – 23:00
 - вторник и четвъртък 19:00 – 23:00
-

Плащане



Заявка за издаване на фактура се приема към момента на записването на съответния курс.

Фактура се издава в рамките на 7 дни от потвърждаване на плащането.

Предстоящи Курсове

[tribe_events_list category="cisco-ccnasec"]

За повече информация използвайте формата за контакт.

Ще се свържем с Вас за потвърждаване на датите.

Предпоставки (Изисквания) за Участие

- Умения и еквивалентни познания на тези, налични в
Свързване на Сиско Мрежови устройства част 1
(ICND1)Работни познания на операционната система
WindowsРаботни познания на Cisco IOS

Курсът подготвя за следните сертификационни нива

- CCNA Security 210-260