NOKIA

Nokia
Service
Routing
Certification

Nokia Network and Service Router Security

Course outline

The Nokia Network and Service Router Security course presents the technology, techniques, and best practices for implementing security in a Service Router-based network. The course begins with an introduction to the security components, security challenges, and security risks, and threats. It then covers in detail various methods, features, and techniques for securing the Nokia Service Router Operating System (SR OS) management plane, control plane, and data plane. Students will participate in many practical hands-on lab exercises throughout the course to ensure implementation-level knowledge of network and router security.

Course number
TTP30096

Duration
4 days

Exam
Nokia Network and Service Router Security (4A0-111)

Credit toward certification
Nokia Service Routing Architect (elective exam)

Recommended pre-requisites

- Nokia IS-IS Routing Protocol or Nokia OSPF Routing Protocol
- Nokia Multiprotocol Label Switching
- Nokia Services Architecture
- Nokia Border Gateway Protocol for Internet Routing

Credit for other IP certifications

If you have already received an IP certification from Cisco orJuniper, and your certification is still valid, you may be eligible to receive credit towards prerequisite written exams in the Nokia Service Routing Certification program. To find out which third-party certifications are eligible for credit, which SRC exam exemptions you may be qualified to receive, and instructions on how to request an exemption, please visit networks.nokia.com/src/exemptions. Please note that your third-party certification must be current/active to receive credit.

Course objectives

After completing the course, students should be able to:

- Define security and its related terms
- Describe the key components of a secure network: authentication, confidentiality, integrity, and availability
- Understand the two types of encryption algorithms
- Understand common security challenges and threats to each layer in the OSI model
- Describe the two management plane access types
- Describe management plane attacks
- Describe and configure various security features to control router access
- Understand how to use filters and logging to restrict management traffic and track user activities
- Explain and implement the configuration management features: configuration rollback, transactional configuration, command accounting, SNMP, and Netconf
- Describe the different control plane threats
- List the various methods and techniques for securing the control plane
- Describe the different features that can be used to protect the CPM, such as CPM filters, CPM queues, and CPU protection
- Describe and configure techniques for Layer 2 VPLS security
- Understand and configure techniques for securing Layer 3 protocols and routing information (IGP, MPLS, Multicast, and BGP)
- Understand different data plane security threats, such as address spoofing, data snooping, and denial of service attacks
- List various techniques that can be used to protect the data plane, such as network monitoring, traffic filters, and IPSec tunnels
- Describe passive and active monitoring and list monitoring options
- Describe and configure local and remote mirroring
- Describe and configure Cflowd
- Understand lawful intercept
- Configure traffic filters
- Describe and configure unicast reverse path forwarding (uRPF) for IPv4/IPv6 protocols
- Describe and configure BGP filters
- Describe and configure BGP remote triggered black hole (RTBH)
- Describe and configure BGP Flowspec
- Describe and configure BGP route origin validation (ROV)
- Describe IPSec protocols (IKE, ESP, AH)
- Understand and configure IPSec tunnels used to protect data integrity

Course modules

- Module 1 – Introduction to Security
- Module 2 – SR OS Management Plane Security
- Module 3 – SR OS Control Plane Security
- Module 4 – SR OS Data Plane Security

Register Now

Nokia Oyj
Karaportti 3
FI-02610 Espoo, Finland
Tel. +358 (0) 10 44 88 000

Document code: (March) CID200515