

Course Outline

Course Name: HCIA-Security Huawei Certified ICT Associate-Security V4.0



Course Code : HW-HCIA-SEC

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
5 Days	Associate	Security	ILT/VILT Theoretic Teaching & Hands-on practice	Huawei Voucher

Introduction

This course covers the fundamental knowledge required to secure enterprise networks, including firewall technologies, NAT, intrusion prevention, encryption, VPNs, and security operations. Learners will gain the skills required to assist in the design, deployment, and maintenance of secure small- and medium-sized enterprise networks.

Audience Profile

- Security operation and maintenance personnel.
- Individuals who want to obtain the HCIA-Security certification.
- Entry-level or junior engineers building cybersecurity skills.
- Cyber security junior engineer who hopes to have information security capabilities.

Prerequisites

- Basic knowledge of TCP/IP networking.
- Basic knowledge of routing and switching.
- General IT knowledge (Security+ recommended but not required).

Course Objectives

- Describe the definition and characteristics of network security
- Describe the development history and trend of network security
- Understand the data definition and transmission process
- Describe the working principles of the TCP/IP protocol stack
- Describe the working principles of common protocols
- Describe common security threats to enterprise networks
- Describe how to cope with common network security threats
- Describe firewall security zones
- Describe the stateful inspection and session mechanisms of the firewall
- Describe the technical background of NAT
- Know the classification and working principles of NAT
- Know the application scenarios of different types of NAT
- Understand the hot standby fundamentals
- Master the basic hot standby configurations
- Describe user authentication technologies
- Describe the different types of intrusion prevention
- Describe the fundamentals of intrusion prevention
- Deploy network antivirus policies
- Development of encryption and decryption technologies
- Processes of various encryption and decryption methods
- Principles of encryption and decryption algorithms
- Describe data communication security technologies
- Describe the PKI certificate system architecture
- Describe the PKI working mechanism
- Application scenarios of encryption technologies
- Configuration methods for different VPN technologies

Training Content

1. Security Information and Security Overview

- **Network Security Concepts and Specifications**
 - Network Security Definition
 - Future Network Security Trends
 - Information Security Standards and Specifications
 - **Network Basics**
 - Network Reference Model
 - Common Network Devices
 - **Common Network Security Threats and Threat Prevention**
 - Overview of Enterprise Network Security Threats
 - Communication Network Security Requirements and Solutions
-

- Zone Border Security Threats and Threat Prevention
- Computing Environment Security Threats and Threat Prevention
- Security Requirements and Solutions of the Management Center

2. Network Security Basis

- **Firewall Security Policies**
 - Firewall Basic Principles
 - Application Scenarios of Firewalls in Cyber Security Solutions
- **Firewall NAT Technologies**
 - Overview of NAT
 - Source NAT
 - Destination NAT
 - Bidirectional NAT
 - NAT ALG and NAT Server
- **Firewall Hot Standby Technologies**
 - Hot Standby Fundamentals
 - Hot Standby Basic Networking and Configuration
- **Firewall User Management Technologies**
 - AAA Principles
 - Firewall User Authentication and Application
- **Firewall IPS**
 - Intrusion Overview
 - Intrusion Prevention
 - Antivirus

3. Application of Encryption and Decryption

- **Fundamentals of Encryption and Decryption Technologies**
 - Encryption/Decryption Technology Development
 - Encryption/Decryption Technology Fundamentals
 - Common Encryption/Decryption Algorithms
 - Hash Algorithms
- **PKI Certificate System**
 - Data Communication Security Technologies
 - PKI System Structure
 - PKI Working Mechanism
- **Encryption Technology Applications**
 - Application of Cryptography
 - VPN Overview
 - VPN Configuration

Associate Certification & Exam

This course prepares delegates for the HCIA-Security certification exam H12-711, validating foundational skills in network security, firewall configuration, VPN technologies, encryption, and security operations.

You need to pass the following exam(s) to obtain the certificate.

- **Certification:** HCIA-Security
- **Exam Code:** H12-711
- **Exam Type:** Written examination
- **Exam Format:** Single-answer Question, Multiple-answer Question, True or false, Short Response Item, Drag and Drop Item