Course Outline

Course Name: HCIP - Huawei Certified ICT Professional Security V4.0

Course Code : HW-HCIP-SEC

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
10 Days	Intermediate	Security	ILT/VILT Training & Hands on Practice	Huawei Voucher

Introduction

The HCIP-Security V4.0 course equips learners with advanced knowledge and capabilities in the architecture design, deployment, optimisation, and O&M of medium- and large-scale enterprise security networks. It covers firewall high reliability technologies, firewall traffic management, firewall virtual systems, firewall intelligent uplink selection, IPsec VPN technology and application, SSL VPN technology and application, cyber attacks and defence, vulnerability defence and penetration testing, content security filtering technologies, emergency response, and network access control.

Audience Profile

- Individuals who want to become network security professionals.
- Cybersecurity engineers and network security engineers responsible for enterprise security solutions.
- Professionals preparing for the HCIP-Security certification.
- Network engineers, system engineers, and IT professionals seeking to advance into security-focused roles.

Prerequisites

- HCIA certification or equivalent knowledge is recommended.
- Basic understanding of TCP/IP, routing, switching, and common network services.
- Foundational knowledge of cybersecurity concepts, firewalls, VPNs, and network access control is beneficial.

Course Objectives

- Describe the principles, networking modes, and application scenarios of firewall high reliability technologies.
- Describe the application scenarios and fundamentals of bandwidth management and quota control policies.
- Master the configuration of firewall traffic management.
- Describe the application scenarios and basic concepts of virtual systems, and configure virtual systems.
- Describe the basic concepts and application scenarios of intelligent uplink selection, and configure intelligent uplink selection.
- Understand the basic principles and typical application scenarios of IPsec VPN.
- Master highly reliable IPsec VPN configuration and troubleshooting methods.
- Understand SSL VPN application scenarios, networking, main functions, and principles.
- Master SSL VPN configuration.
- Describe the principles of common single-packet attacks and DDoS attacks.
- Describe the principles of defending against single-packet attacks and DDoS attacks, including anti-DDoS solutions and related defence principles.
- Describe the cyber kill chain and the impact of vulnerabilities, and master vulnerability defence measures.
- Describe the technical background and basic principles of content security filtering technologies, and configure content security filtering technologies.
- Describe the basic concepts, handling process, and related technologies of cybersecurity emergency response.
- Describe the basic concepts of NAC, user identity authentication, and common access authentication modes.
- Configure user access authentication.
- Apply various network security technologies to design, deploy, and operate network security solutions.
- Be familiar with network security O&M.

Course Content

Module 1: Secure Communication Network

- **Overview of Cyber Security Certification**
    - Capability models for cybersecurity engineers
    - Cyber Security Certification overview
- **Firewall High Reliability Technologies**

  - Overview of firewall high reliability technologies
  - Firewall hot standby
  - Firewall link high reliability
  - Hot standby version upgrade and troubleshooting
- **Firewall Traffic Management**
  - Firewall bandwidth management
  - Firewall quota control policies
  - Example for configuring traffic management
- **Firewall Virtual System**
  - Virtual system overview
  - Basic concepts of virtual systems
  - Communication between virtual systems
  - Virtual system configuration
- **Firewall Intelligent Uplink Selection**
  - Overview of intelligent uplink selection
  - Principles of intelligent uplink selection
  - Configuration of intelligent uplink selection
- **IPsec VPN Technology and Application**
  - Basic principles of IPsec VPN
  - Application scenarios of IPsec VPN
  - High reliability of IPsec VPN
  - Troubleshooting of IPsec VPN
- **SSL VPN Technology and Application**
  - Overview of SSL VPN
  - Service functions of SSL VPN
  - Examples for configuring SSL VPN
  - SSL VPN troubleshooting

Module 2: Security Zone Border Protection

- **Cyber Attacks and Defence**
  - Firewall attack defence technologies
  - Single-packet attack defence
  - DDoS mitigation
  - Anti-DDoS
- **Vulnerability Defence and Penetration Testing**
  - Vulnerability concepts
  - Vulnerability defence
  - Penetration testing
- **Content Security Filtering Technologies**
  - Overview of content security filtering technologies
  - Principles of content security filtering technologies
  - Examples for configuring content security filtering technologies

Module 3: Security Management and Operations

- **Emergency Response**
  - Emergency response overview
  - Emergency response process
  - Emergency response technologies and cases
- **Network Access Control**
  - Overview of NAC
  - User identity authentication
  - Access authentication
  - NAC configuration
- **Comprehensive Cases of Enterprise Network Security**
  - Overview of enterprise network security requirements
  - Enterprise network security solution design and deployment
  - Enterprise network security troubleshooting

Professional Certification & Exam

This course prepares delegates for the HCIP-Security certification exam H12-725, validating advanced skills in enterprise security architecture, firewall technologies, VPN deployment, threat defence, and security operations.