Course Outline

Course Name: Huawei Certified ICT Professional Security

Course Code: HW-HCIP-SEC

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
10 Days	Professional	Security	VITL/In Class	Huawei Learning Vouchers

Introduction

The updated HCIP - Security version 4.0 course aims to equip delegates with knowledge around architecture design, deployment and O&M capabilities of medium and large enterprise security networks.
You will learn Firewall high reliability technologies, Firewall traffic management, Firewall virtual system, Firewall intelligent uplink selection, IPSec VPN technology and application, SSL VPN technology and application, cyber attacks and defense, vulnerability defense and penetration testing, content security filtering technologies, emergency response and network access control.

Target Audience

- Those pursuing senior network security engineering or cyber security engineering roles.
- Those pursiong HCIP Security certification.

Prerequisites

Before attending this course, delegates must have successfully completed or have demonstrated industry knowledge of objectives covered in the HCIA Security certification course.

Course Objectives

On completion of this program, the participants should be able to:

- Describe the principles of firewall high reliability technologies
- Understand the high reliability networking mode of the firewall
- Describe the application scenarios of firewall high reliability technologies
- Describe the application scenarios of bandwidth management
- Describe the fundamentals of bandwidth management
- Describe the application scenarios of quota control policies
- Describe the fundamentals of quota control policies
- Master the configurations of firewall traffic management
- Describe the application scenarios of virtual systems
- Describe the basic concepts of virtual systems
- Master how to configure virtual systems
- Describe basic concepts of intelligent uplink selection
- Describe the application scenarios of intelligent uplink selection
- Master the configuration procedure of intelligent uplink selection
- Understand the basic principles of IPsec VPN
- Understand the typical application scenarios of IPsec VPN
- Master the highly reliable IPsec VPN configuration method
- Master IPsec VPN troubleshooting method
- Understand application scenarios of SSL VPN
- Master the main functions and principles of SSL VPN
- Understand the SSL VPN networking
- Master the configuration of SSL VPN
- Describe the principles of common single-packet attacks
- Describe the principles of common DDoS attacks
- Describe the principles of defending against single-packet attacks
- Describe the principles of defending against DDoS attacks
- Describe the anti-DDoS solution and related defense principles
- Describe the cyber kill chain
- Describe the harm of vulnerabilities
- Master vulnerability defense measures
- Describe the technical background of the content security filtering technologies
- Describe basic principles of content security filtering technologies
- Master the configuration of content security filtering technologies
- Describe the basic concepts of cyber security emergency response
- Describe the handling process of cyber security emergency response
- Understand technologies related to cyber security emergency response
- Describe the basic concepts of NAC
- Describe the working principles of user identity authentication
- Describe common access authentication modes and their working principles
- Configure user access authentication
- Apply various network security technologies
- Design a network security solution
- Deploy a network security solution
- Be familiar with network security O&M

Course Content

Lesson 1: Secure communication network

- Overview of Cyber Security Certification
- Capability Models for Cyber Security Engineers
- Cyber Security Certification 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 the SSL VPN
- SSL VPN Troubleshooting

Lesson 2: Security zone border

- Cyber Attacks and Defense
- Firewall Attack Defense Technologies
- Single-Packet Attack Defense
- DDoS Mitigation
- Anti-DDoS Vulnerability Defense and Penetration Testing
- Vulnerability
- Vulnerability Defense
- 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

Lesson 3: Security management center

- 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

ASSOCIATED CERTIFICATIONS & EXAM

This course will prepare delegates to take the HCIP Security version 4.0 Certification Exam # H12-725.