HCIP-Security V4.0 Exam Outline

Huawei Certification HCIP-Security Certification Exam

Certification	Exam Code	Exam Name	Exam Format	Language	Exam Cost	Exam Duration	Pass Score/ Total Score
HCIP-Security	H12-725	HCIP-Security V4.0	True-false Question, Single Answer, Multiple Answer, Fill in the bank answers, Drag and drop item	ENU/CHS	300USD	90min	600/1000

Exam Content

The HCIP-Security V4.0 exam content covers 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.

Knowledge Module Percentage

Key Module	Exam Percentage
Firewall High Reliability Technologies	7%
Firewall Traffic Management	5%
Firewall Virtual System	6%
Firewall Intelligent Uplink Selection	6%
IPSec VPN Technology and Application	13%
SSL VPN Technology and Application	9%
Cyber Attacks and Defense	12%
Vulnerability Defense and Penetration Testing	10%
Content Security Filtering Technologies	12%
Emergency Response	5%
Network Access Control	15%

Knowledge points

1. Firewall High Reliability Technologies

1.1 Overview of Firewall High Reliability Technologies

1.2 Firewall Hot Standby

1.3 Firewall Link High Reliability

1.4 Hot Standby Version Upgrade and Troubleshooting

2. Firewall Traffic Management

2.1 Firewall Bandwidth Management

2.2 Firewall Quota Control Policies

2.3 Example for Configuring Traffic Management

3. Firewall Virtual System

3.1 Virtual System Overview

3.2 Basic Concepts of Virtual Systems

3.3 Communication Between Virtual Systems

3.4 Virtual System Configuration

4. Firewall Intelligent Uplink Selection

4.1 Overview of Intelligent Uplink Selection

4.2 Principles of Intelligent Uplink Selection

4.3 Configuration of Intelligent Uplink Selection

5. IPsec VPN Technology and Application

5.1 Basic Principles of IPsec VPN

5.2 Application Scenarios of IPsec VPN

5.3 High Reliability of IPsec VPN

5.4 Troubleshooting of IPsec VPN

6. SSL VPN Technology and Application

6.1 Overview of SSL VPN

6.2 Service Functions of SSL VPN

6.3 Examples for Configuring the SSL VPN

6.4 SSL VPN Troubleshooting

7. Cyber Attacks and Defense

7.1 Firewall Attack Defense Technologies

7.2 Single-Packet Attack Defense

7.3 DDoS Mitigation

7.4 Anti-DDoS

8. Vulnerability Defense and Penetration Testing

8.1 Vulnerability

8.2 Vulnerability Defense

8.3 Penetration Testing

9. Content Security Filtering Technologies

9.1 Overview of Content Security Filtering Technologies

9.2 Principles of Content Security Filtering Technologies

9.3 Examples for Configuring Content Security Filtering Technologies

10. Emergency Response

10.1 Emergency Response Overview

10.2 Emergency Response Process

10.3 Emergency Response Technologies and Cases

11. Network Access Control

11.1 Overview of NAC

11.2 User Identity Authentication

11.3 Access Authentication

11.4 NAC Configuration

NOTE

The content mentioned in this document is a general exam guide only. The exam may also contain more specific or related content that is not mentioned above.

Reference

HCIP-Security V4.0 Course

Recommended Training

HCIP-Security V4.0 Training