

Exam requirements

Security Certified Network Specialist (SCNS.EN)

Publication date 01.12.2009

Start date 01.06.2009

Summary The Tactical Perimeter Defense (TPD) exam SC0-451 tests the knowledge and skills for the Security Certified Network Specialist (SCNS) certification. It focuses on the critical defense technologies that are the foundation of securing network perimeters, such as firewalls, intrusion detection, and router security. The Tactical Perimeter Defense exam covers the following subjects, validating the foundation skills required by today's Security Professionals in order to work with and implement real-world security technology:

- Network Defense Fundamentals.
- Advanced TCP/IP
- Routers and Access Control Lists
- Designing Firewalls
- Configuring Firewalls
- Implementing IPsec and VPNs
- Designing an Intrusion Detection System (IDS)
- Configuring IDS
- Securing Wireless Networks

Target group IT professionals who are entering the world of security. Those who have to work with, and implement, real world security technology.

Context The SCNS module fits in EXIN's Information Security program, which has a managerial and a technical stream. SCNS is positioned in the technical stream of the qualification scheme. The Security Certified Program in the technical stream offers three certifications to validate IT professionals' security skill sets, of which SCNS is the first. SCNS is a required pre-requisite for going further towards the SCNP and SCNA certifications.

Prerequisites Security+ certification or equivalent work experience is recommended.
Note that SCP and EXIN are not affiliated with the Security+ certification from CompTIA.
The SCNS Tactical Perimeter Defense Course, delivered by an SCP Authorized Training Partner, is recommended.
As the security industry moves quickly, skills require consistent validation. The SCNS credential is valid for two years from the pass date. Recertification is required to maintain good standing.

Practical assignment	Not applicable	
Examination details	Examination type:	Computer-based or paper-based multiple-choice and multiple-response questions
	Time allotted for examination:	90 minutes
	Number of multiple-choice/response questions:	60
	Pass mark:	75% (45 marks out of 60 marks)
	Open book:	no
	Electronic equipment permitted:	no

Sample questions A sample exam (cd-rom or online usage) can be bought from MeasureUp at www.measureup.com.

Exam requirements	1. Network Defense Fundamentals	5%
	2. Hardening Routers and Access Control Lists	10%
	3. Implementing IPSec and Virtual Private Networks	10%
	4. Advanced TCP/IP	15%
	5. Securing Wireless Networks	15%
	6. Designing and Configuring Intrusion Detection Systems	20%
	7. Designing and Configuring Firewall Systems	25%

Examination session	Referral to literature and notes is not permitted.
----------------------------	---

Specification of the exam requirements

1. Network Defense Fundamentals	<ul style="list-style-type: none"> 1.1 Examine Network Defense Fundamentals 1.2 Identify Network Defense Technologies 1.3 Examine Access Control Methods 1.4 Define the Principles of Network Auditing 1.5 Identify the Impact of Defense
2. Hardening Routers and Access Control Lists	<ul style="list-style-type: none"> 2.1 Implement Fundamental Cisco Router Security 2.2 Describe the Routing Process 2.3 Remove Unwanted Protocols and Services 2.4 Create and Implement Access Control Lists 2.5 Configure Cisco Router Logging
3. Implementing IPSec and Virtual Private Networks	<ul style="list-style-type: none"> 3.1 IPSec Fundamentals 3.2 Implement IPSec on Windows Server 2003 3.3 Identify Core VPN Concepts 3.4 Examine VPN Design and Architecture 3.5 Implement a VPN using Windows Server 2003
4. Advanced TCP/IP	<ul style="list-style-type: none"> 4.1 Examine the Core Concepts of TCP/IP

	4.2 Identify and Describe Packet Headers
	4.3 Examine the Session Setup and Teardown Process
5. Securing Wireless Networks	5.1 Describe Wireless Networking Fundamentals
	5.2 Implement Wireless Security Solutions
	5.3 Configure Wireless Auditing
	5.4 Identify Wireless PKI Solutions
6. Designing and Configuring Intrusion Detection Systems	6.1 Identify the Goals of an IDS
	6.2 Examine Host-Based Intrusion Detection
	6.3 Examine Network-Based Intrusion Detection
	6.4 Describe IDS Log Analysis
	6.5 Describe Methods of Using an IDS
7. Designing and Configuring Firewall Systems	7.1 Identify Firewall Components
	7.2 Create a Firewall policy
	7.3 Define Firewall rule Sets and Packet Filters
	7.4 Examine the Proxy Server
	7.5 Examine the Bastion Host
	7.6 Describe a Honeypot
	7.7 Install and Configure ISA Server 2006
	7.8 Install and Configure IPTables

List of Basic Concepts

This section contains the terms with which candidates should be familiar. Terms are listed in alphabetical order.

- Access Control List (ACL)
- Address Conversion
- Anti-spoofing Logging
- Authentication
- Authorization
- Bastion Host
- Buffered Logging
- Caching
- Chain Management
- Challenge Response
- Cisco Discovery Protocol (CDP)
- Datagram
- File Transfer Protocol (FTP)
- Firewall
- Hardening
- Honeypot
- Internet Control Message Protocol (ICMP)
- Intrusion Detection System (IDS)
- Host-based
- Network-based
- IPSec

- Login Banners
- Media Access Control (MAC)
- Network Auditing
- Non-repudiation
- Packet Filters
- Packet Fragmentation
- Proxy Server
- Routing Information Protocol (RIP)
- Rule Element
- Secure Shell (SSH)
- Snort
- Subnetting
- TCP/IP
- Three-way Handshake
- Token
- Tunneling Protocol
- User Datagram Protocol (UDP)
- Virtual Private Network (VPN)
- Wildcard Mask
- Wireshark

Literature

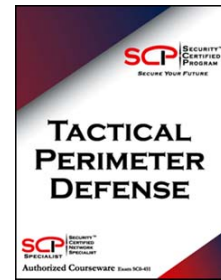
A

SCP

Tactical Perimeter Defense

SCP Authorized Courseware for the Security Certified Network Specialist module

www.securitycertified.net



Exam requirement	Literature
1	A: Chapter 1
2	A: Chapter 3
3	A: Chapter 6
4	A: Chapter 2
5	A: Chapter 9
6	A: Chapter 7,8
7	A: Chapter 4,5

Copyright © 2009 EXIN

All rights reserved. No part of this publication may be published, reproduced, copied or stored in a data processing system or circulated in any form by print, photo print, microfilm or any other means without written permission by EXIN.

EXIN, Examination Institute for Information Science, is the certification organization that independently develops and delivers the certifications for the Security Certified Program.