

# Tactical Perimeter Defense (SCP-SCNS)



## Overview

The Security Certified Network Specialist (SCNS) program focuses on the critical defensive technologies that are the foundation of securing network perimeters, such as firewalls, intrusion detection, and router security. The up-to-date security lessons and the hands-on labs in the SCNS courseware bring the security networking world to the candidates. A heterogeneous environment is put in place within the classroom environment (using Windows Server, Linux & CISCO) to enable a participant to have a real world hands-on experience.

To prepare for the examination, candidates are recommended to attend training with an SCP Authorized Training Partner (ATP). The course to prepare for the exam is called, Tactical Perimeter Defense (TPD). Course details can be found here: [Tactical Perimeter Defense](#).

The SCNS certification requires the passing of one exam (number SC0-451), details of the exam can be found here: [Tactical Perimeter Defense, SC0-451](#).

The exam is designed to validate the essential perimeter security skills, including: Network Defense Fundamentals, Hardening Routers and ACLs, Implementing IPsec and VPNs, Advanced TCP/IP, Securing Wireless Networks, Designing and Configuring Intrusion Detection Systems, and Designing and Configuring Firewall Systems.

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.

Prerequisite for this certification is Security+ or equivalent experience. For further information on the Security+ program, click here to visit the CompTIA website. SCP is not affiliated with, nor owns any part of, the Security+ certification.

## SCP Certification Roadmap:



## Exams

Related Exam: SC0-451 Tactical Perimeter Defense

## Related Course

After:  
Strategic Infrastructure Security (SCP-SCNP)  
Mile2 & Shon Harris Blended CISSP (M2-CISSP)

## REGISTRATION AND INFORMATION

education@ecs.com.sg  
TEL: (65) 6393-4737 (65) 6393-4741  
FAX: (65) 6294-4097



# Tactical Perimeter Defense (SCP-SCNS)

## Course Outlines:

### LESSON 1: NETWORK DEFENSE FUNDAMENTALS

- Network Defense
- Defensive Technologies
- Objectives of Access Control
- The Impact of Defense
- Network Auditing Concepts

#### TASKS

Identifying Non-repudiation Issues, Describing the Layers of a Defended Network,  
Describing the Challenge Response Token Process,  
Describing the Problems of  
Additional Layers of Security, Describing Network Auditing

### LESSON 2: ADVANCED TCP/IP

- TCP/IP Concepts
- Analyzing the Three-way Handshake
- Capturing and Identifying IP Datagrams
- Capturing and Identifying ICMP Messages
- Capturing and Identifying TCP Headers
- Capturing and Identifying UDP Headers
- Analyzing Packet Fragmentation
- Analyzing an Entire Session

#### TASKS

- Layering and Address Conversions, Routers and Subnetting, Using Network Monitor,
- Installing and Starting Wireshark, Using Wireshark, Analyzing the Three-way Handshake, Analyzing the Session Teardown Process, Capturing and Identifying IP Datagrams, Capturing and Identifying ICMP Messages, Capturing and Identifying TCP Headers, Working with UDP Headers, Analyzing Fragmentation, Performing a Complete ICMP Session Analysis, Performing a Complete FTP Session Analysis

### LESSON 3: ROUTERS AND ACCESS CONTROL LISTS

- Fundamental Cisco Security
- Authentication and Authorization
- Configuring Access Passwords
- Routing Principles
- Removing Protocols and Services
- Creating Access Control Lists
- Implementing Access Control Lists
- Logging Concepts

#### TASKS

- Configuring Passwords, Configuring Login Banners, Configuring SSH on a Router,
- Configuring the SSH Client, Performing IP and MAC Analysis, Viewing a RIP Capture,
- Viewing a RIPv2 Capture, Turning Off CDP, Hardening ICMP, Removing Unneeded Services, Creating Wildcard Masks, Creating Access Control Lists, Configuring Buffered Logging, Configuring Anti-spoofing Logging

### LESSON 4: DESIGNING FIREWALLS

- Firewall Components
- Create a Firewall Policy
- Rule Sets and Packet Filters
- Proxy Server
- The Bastion Host
- The Honeypot

#### TASKS

- Firewall Planning, Creating a Simple Firewall Policy, Firewall Rule Creation, Diagram
- the Proxy Process, Describing a Bastion Host, Honeypot Configuration,

### LESSON 5: CONFIGURING FIREWALLS

- Understanding Firewalls
- Configuring Microsoft ISA Server 2006
- IPTables Concepts
- Implementing Firewall Technologies

#### TASKS

- Install Microsoft ISA Server 2006, Exploring the Microsoft ISA Server 2006 Interface,
- Exporting the Default Configuration, Creating a Basic Access Rule, Creating a Protocol Rule Element, Creating a User Rule Element, Creating a Content Group Rule Element,
- Creating and Modifying Schedule Rule Elements, Using Content Types and Schedules in Rules, Creating a Network Rule Element, Configuring a Web Publishing Rule, Enabling and Configuring Caching, Install Second Microsoft Loop Back Adapter and Assign an IP Address, Working with Alerts, Working with Reports, Configuring Logging Option,
- Securing ISA Server 2006 with the Security Configuration Wizard, Configuring Packet Prioritization, Uninstalling ISA Server 2006, Working with Chain Management

## REGISTRATION AND INFORMATION

education@ecs.com.sg  
TEL: (65) 6393-4737 (65) 6393-4741  
FAX: (65) 6294-4097

# Tactical Perimeter Defense (SCP-SCNS)

## LESSON 6: IMPLEMENTING IPSEC AND VPNS

- Internet Protocol Security
- IPsec Policy Management
- IPsec AH Implementation
- Combining AH and ESP in IPsec
- VPN Fundamentals
- Tunneling Protocols
- VPN Design and Architecture
- VPN Security
- Configuring a VPN

### TASKS

Describing the Need for IPsec, Examining the MMC, Identifying Default IPsec Security Policies, Saving a Customized MMC, Examining Security Methods, Examining Policy Rules, Creating the 1\_REQUEST\_AH(md5)\_only Policy, Editing the 1\_REQUEST\_AH(md5)\_only Policy, Configuring the Policy Response, Configuring the Second Computer, Setting Up the FTP Process, Implementing the 1\_REQUEST\_AH(md5)\_only Policy, Analyzing the Request-only Session, Configuring a Request-and-Respond IPsec Session, Analyzing the Request-and-Respond Session, Creating the 5\_REQUEST\_AH(md5)+ESP(des) IPsec Policy and the Response Policy, Creating the 5\_RESPONSE\_AH(md5)+ESP(des) IPsec Policy, Configuring & Analyzing an IPsec Session Using AH & ESP, Implementing the 7\_REQUIRE\_AH(sha) +ESP(sha+3des) Policy, Implementing the 7\_RESPONSE\_AH(sha) +ESP(sha+3des) Policy, Implementing and Analyzing an AH(sha) and ESP(sha+3des) IPsec Session, Assigning Tunneling Protocols, Assigning Additional Tunneling Protocols, Examining VPN-related RFCs, Viewing Firewall-related RFCs, Configuring the VPN Server, Configuring VPN Clients, Establish the VPN, Restoring the Classroom Setup

## LESSON 7: DESIGNING AN INTRUSION DETECTION SYSTEM

- The Goals of an Intrusion Detection System
- Technologies and Techniques of Intrusion Detection
- Host-based Intrusion Detection
- Network-based Intrusion Detection
- The Analysis
- How to Use an IDS
- What an IDS Cannot Do

### TASKS

- Describing Alarms, Discussing IDS Concepts, Describing Centralized Host-based
- Intrusion Detection, Discussing Sensor Placement, Discussing Data Analysis, Discussing
- Intrusion Detection Uses, Discussing Incident Investigation.

## LESSON 8: CONFIGURING AN IDS

- Snort Foundations
- Snort Installation
- Snort as an IDS
- Configuring Snort to Use a Database
- Running an IDS on Linux

### TASKS

- Installing Snort, Initial Snort Configuration, Capturing Packets with Snort, Capturing
- Packet Data with Snort, Logging with Snort, Creating a Simple Ruleset, Testing the
- Ruleset, Examining Pre-configured Rules, Examining DDoS Rules, Examining Backdoor
- Rules, Examining Web Attack Rules, Examining IIS Rules, Editing Snort.Conf,
- Installing MySQL, Creating the Snort Database, Creating MySQL User Accounts,
- Testing the New Configuration, Configuring Snort as a Service, Installing LAMP
- Components, Apache and PHP Test, Configure Snort on Linux, Configuring MySQL for
- Snort, Testing Snort Connectivity to the Database, Downloading ADOdb and BASE,
- Installing ADOdb and BASE, Configuring BASE, Configuring the Firewall to Allow
- HTTP, Generating Portscan Snort Events, Generating Web Snort Events

## LESSON 9: SECURING WIRELESS NETWORKS

- Wireless Networking Fundamentals
- Wireless LAN (WLAN) Fundamentals
- Wireless Security Solutions
- Wireless Auditing
- Wireless Trusted Networks

### TASKS

- Examining Satellite Orbits, Choosing a Wireless Media, Installing the Linksys WPC54G
- WNIC, Installing the Netgear WPN511, Enabling the Ad-Hoc Network, Installing the
- Linksys WAP54G Access Point, Configuring the Linksys Client, Configuring the
- Netgear Client, Installing the Netgear WPN824 Access Point, Configuring WEP on the
- Network Client, Configure WPA2 on the Access Point, Configuring WPA2 on the
- Network Client, Installing NetStumbler, Identifying Wireless Networks, Installing
- OmniPeek Personal, Viewing OmniPeek Personal Captures, Viewing Live OmniPeek
- Personal Captures, Analyze Upper Layer Traffic, Decrypting WEP, Choosing a Wireless
- Trusted Network

## REGISTRATION AND INFORMATION

education@ecs.com.sg  
 TEL: (65) 6393-4737 (65) 6393-4741  
 FAX: (65) 6294-4097