

Securing Cisco Networks with Open Source Snort (SSFSNORT) v2.0

What you'll learn in this course

The **Securing Cisco Networks with Open Source Snort (SSFSNORT) v2.0** course shows you how to deploy a network intrusion detection system based on Snort. Through a combination of expert instruction and hands-on practice, you will learn how to install, configure, operate, and manage a Snort system, rules writing with an overview of basic options, advanced rules writing, how to configure Pulled Pork, and how to use OpenAppID to provide protection of your network from malware. You will learn techniques of tuning and performance monitoring, traffic flow through Snort rules, and more.

Course duration

- Instructor-led classroom: 4 days in the classroom with hands-on lab practice
- Instructor-led virtual classroom: 4 days of web-based classes with hands-on lab practice

How you'll benefit

This course will help you:

- Learn how to implement Snort, an open-source, rule-based, intrusion detection and prevention system
- Gain leading-edge skills for high-demand responsibilities focused on security

Who should enroll

This course is for technical professionals who need to know how to deploy open source, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), and how to write Snort rules.

- Security administrators
- Security consultants
- Network administrators
- System engineers
- Technical support personnel
- Channel partners and resellers

How to enroll

- For instructor-led training, visit the [Cisco Learning Locator](#)
- For private group training, visit [Cisco Private Group Training](#)
- For digital library access, visit [Cisco Platinum Learning Library](#)
- For e-learning volume discounts, contact ask_cpll@cisco.com

Technology areas

- Security

Course details

Objectives

After taking this course, you should be able to:

- Describe Snort technology and identify resources available for maintaining a Snort deployment
- Install Snort on a Linux-based operating system
- Describe the Snort operation modes and their command-line options
- Describe the Snort intrusion detection output options
- Download and deploy a new rule set to Snort
- Describe and configure the snort.conf file
- Configure Snort for inline operation and configure the inline-only features
- Describe the Snort basic rule syntax and usage
- Describe how traffic is processed by the Snort engine
- Describe several advanced rule options used by Snort
- Describe OpenAppID features and functionality
- Describe how to monitor Snort performance and how to tune rules

Prerequisites

To fully benefit from this course, you should have:

- Technical understanding of TCP/IP networking and network architecture
- Proficiency with Linux and UNIX text editing tools (vi editor is suggested but not required)

Outline

- Introduction to Snort Technology
- Snort Installation
- Snort Operation
- Snort Intrusion Detection Output
- Rule Management
- Snort Configuration
- Inline Operation and Configuration
- Snort Rule Syntax and Usage
- Traffic Flow Through Snort Rules
- Advanced Rule Options
- OpenAppID Detection
- Tuning Snort

Lab outline

- Connecting to the Lab Environment
- Snort Installation
- Snort Operation
- Snort Intrusion Detection Output
- Pulled Pork Installation
- Configuring Variables
- Reviewing Preprocessor Configurations
- Inline Operations
- Basic Rule Syntax and Usage
- Advanced Rule Options
- OpenAppID
- Tuning Snort




Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Course content is dynamic and subject to change without notice.