

# Securing Cisco Networks with Snort Rule Writing Best Practices (SSF Rules) v2.1

## What you'll learn in this course

The **Securing Cisco Networks with Snort Rule Writing Best Practices (SSF Rules) v2.1** course shows you how to write rules for Snort, an open-source intrusion detection and prevention system. Through a combination of expert-instruction and hands-on practice, this course provides you with the knowledge and skills to develop and test custom rules, standard and advanced rules-writing techniques, how to integrate OpenAppID into rules, rules filtering, rules tuning, and more. The hands-on labs give you practice in creating and testing Snort rules.

## Course duration

- Instructor-led classroom: 3 days in the classroom with hands-on lab practice
- Instructor-led virtual classroom: 3 days of web-based classes with hands-on lab practice
- E-learning: Equivalent to 3 days of classroom instruction

## How you'll benefit

This course will help you:

- Gain an understanding of characteristics of a typical Snort rule development environment
- Gain hands-on practices on creating rules for Snort
- Gain knowledge in Snort rule development, Snort rule language, standard and advanced rule options

## Who should enroll

This course is for technical professionals to gain skills in writing rules for Snort-based Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). The primary audience includes:

- Security administrators
- Security consultants
- Network administrators
- System engineers
- Technical support personnel using open source IDS and IPS
- Channel partners and resellers

## How to enroll

### Instructor-led training

- Find a class at the [Cisco Learning Locator](#)
- Arrange training at your location through [Cisco Private Group Training](#)

### E-learning

- To buy a single e-learning license, visit the [Cisco Learning Network Store](#).
- For more than one license, or a learning library subscription, contact us at [learning-bdm@cisco.com](mailto:learning-bdm@cisco.com).

## Technology areas

- Security

## Course details

### Objectives

After taking this course, you should be able to:

- Describe the Snort rule development process
- Describe the Snort basic rule syntax and usage
- Describe how traffic is processed by Snort
- Describe several advanced rule options used by Snort
- Describe OpenAppID features and functionality
- Describe how to monitor the performance of Snort and how to tune rules

### Prerequisites

To fully benefit from this course, you should have:

- Basic understanding of networking and network protocols
- Basic knowledge of Linux command-line utilities
- Basic knowledge of text editing utilities commonly found in Linux
- Basic knowledge of network security concepts
- Basic knowledge of a Snort-based IDS/IPS system

### Outline

- Introduction to Snort Rule Development
- Snort Rule Syntax and Usage
- Traffic Flow Through Snort Rules
- Advanced Rule Options
- OpenAppID Detection
- Tuning Snort

## Lab outline

- Connecting to the Lab Environment
- Introducing Snort Rule Development
- 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](http://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.

© 2021 Cisco and/or its affiliates. All rights reserved.

SSFRULES\_2.1 C22-743269-02 01/21