

Course : Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPF)

Official course, partial preparation for exam 300-710 SNCF

Practical course - 5d - 35h00 - Ref. RJK

Price : 4350 € E.T.

★★★★★ 5 / 5

Nouvelle édition

With this training course you will learn how to implement and configure Cisco Secure Firewall Threat Defense for deployment as a next-generation firewall at the edge of the Internet. You'll learn about Cisco Secure Firewall architecture and deployment, basic configuration, packet handling and advanced options, as well as troubleshooting Cisco Secure Firewall administration.

Teaching objectives

At the end of the training, the participant will be able to:

- ✓ Describe Cisco Secure Firewall threat defense
- ✓ Describe Cisco Secure Firewall Threat Defense deployment options
- ✓ Configuring initial Cisco Secure Firewall Threat Defense settings
- ✓ Configuring high availability on Cisco Secure Firewall Threat Defense
- ✓ Configure an access control policy on Cisco Secure Firewall Threat Defense
- ✓ Configuring intrusion policy on Cisco Secure Firewall Threat Defense
- ✓ Configuring file policy on Cisco Secure Firewall Threat Defense
- ✓ Configuring security intelligence on Cisco Secure Firewall Threat Defense
- ✓ Perform basic threat analysis with Cisco Secure Firewall Management Center
- ✓ Perform basic traffic flow troubleshooting on Cisco Secure Firewall Threat Defense

Intended audience

Network security engineers. Administrators.

PARTICIPANTS

Network security engineers.
Administrators.

PREREQUISITES

Understanding of TCP/IP networks and basic routing protocols, as well as firewall, VPN and IPS concepts.

TRAINER QUALIFICATIONS

The experts who lead the training courses are specialists in the subjects covered. They are approved by the publisher and certified for the course. They have also been validated by our teaching teams in terms of both professional knowledge and teaching skills for each course they teach. They have at least three to ten years of experience in their field and hold or have held positions of responsibility in companies.

ASSESSMENT TERMS

Assessment of targeted skills prior to training.

Assessment by the participant, at the end of the training course, of the skills acquired during the training course.

Validation by the trainer of the participant's learning outcomes, specifying the tools used: multiple-choice questions, role-playing exercises, etc.

At the end of each training course, ITTCERT provides participants with a course evaluation questionnaire, which is then analysed by our teaching teams. Participants also complete an official evaluation of the publisher.

An attendance sheet for each half-day of attendance is provided at the end of the training course, along with a certificate of completion if the participant has attended the entire session.

Prerequisites

Understanding of TCP/IP networks and basic routing protocols, as well as firewall, VPN and IPS concepts.

Practical details

Teaching methods

Training in French. Official course material in English.

Course schedule

1 Official program

- Introducing Cisco Secure Firewall Threat Defense.
- Describe deployment options for Cisco Secure Firewall Threat Defense.
- Describe Cisco Secure Firewall Threat Defense management options.
- Configure basic network parameters on Cisco Secure Firewall Threat Defense.
- Configure high availability on Cisco Secure Firewall Threat Defense.
- Configure automatic NAT on Cisco Secure Firewall Threat Defense.
- Describe packet and policy processing on Cisco Secure Firewall Threat Defense.
- Configure the discovery policy on Cisco Secure Firewall Threat Defense.
- Configure the pre-filtering policy on Cisco Secure Firewall Threat Defense.
- Configure access control policy on Cisco Secure Firewall Threat Defense.
- Configure Security Intelligence on Cisco Secure Firewall Threat Defense.
- Configure file policy on Cisco Secure Firewall Threat Defense.
- Configure intrusion policy on Cisco Secure Firewall Threat Defense.
- Run a basic threat analysis on the Cisco Secure Firewall management center.
- Manage the Cisco Secure Firewall threat defense system.
- Troubleshoot one of the basic traffic flows.
- Manage Cisco Secure Firewall Threat Defense devices.

2 Official practical work

- Carry out initial device configuration.
- Configure high availability.
- Configure network address translation.
- Configure network discovery.
- Configure prefilter and access control policy.
- Configure security intelligence.
- Implement file control and advanced malware protection.
- Configure Cisco Secure IPS.
- Analyze in detail using the Firewall Management Center.
- Manage the Cisco Secure Firewall threat defense system.
- Basic troubleshooting principles for secure firewalls.
- Configure managed devices using Cisco Secure Firewall Device Manager.

TEACHING AIDS AND TECHNICAL RESOURCES

The teaching resources used are the publisher's official materials and practical exercises.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training course.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you have specific accessibility requirements? Contact Ms FOSSE, disability advisor, at the following address: psh-accueil@orsys.fr so that we can assess your request and its feasibility.

Options

Certification : 340 € H.T.

For Cisco Certified Network Professional Security (CCNP Security) certification, passing the 350-701 SCOR exam is required, as well as passing a concentration exam such as the 300-710 Securing Networks with Cisco Firepower (SNCF) concentration exam.

[Comment passer votre examen ?](#)

The certification option comes in the form of a voucher or invitation that will allow you to take the exam at the end of the training course.

Dates and locations

REMOTE CLASS

2026 : 12 Oct., 16 Nov.