Course : Advanced Techniques for Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPA)

Official course, partial preparation for exam 300-710 SNCF

Practical course - 5d - 35h00 - Ref. PPX
Price : 4350 € E.T.

Nouvelle édition

With this course you'll learn how to deploy and configure Cisco Secure Firewall Threat Defense and its features as a data center or Internet edge network firewall with VPN support. You'll also learn how to configure identity-based policies, SSL decryption, remote access and site-to-site VPNs, as well as advanced features like IPS, event management, system integrations, advanced troubleshooting, automation via API, and Cisco Secure Firewall configuration migration (ASA).

Teaching objectives

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

- Describe Cisco Secure Firewall Threat Defense
- Describe advanced deployment options for Cisco Secure Firewall Threat Defense
- Configuring dynamic routing on Cisco Secure Firewall Threat Defense
- Configure advanced network address translation (NAT)
- Configure SSL decryption policy
- Deploy a site-to-site IPsec VPN and a remote access VPN
- Deploy identity-based policies
- Deploy advanced access control settings (ACP)
- Troubleshoot traffic flow using advanced options
- Describe advanced event management on Cisco Secure Firewall Threat Defense

Intended audience

System installers, system integrators, system administrators, network administrators and solution designers.

PARTICIPANTS

System installers, system integrators, system administrators, network administrators and solution designers.

PREREQUISITES

Knowledge of TCP/IP and routing protocols. Familiarity with course content "Securing Internet Edge with Cisco Secure Firewall Threat Defense".

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

Knowledge of TCP/IP and routing protocols. Familiarity with course content "Securing Internet Edge with Cisco Secure Firewall Threat Defense".

Practical details

Teaching methods

Training in French. Official course material in English.

Course schedule

1 Official program

- Introduction to Cisco Secure Firewall Threat Defense.
- Describe advanced deployment options for Cisco Secure Firewall Threat Defense.
- Configure advanced device settings on Cisco Secure Firewall Threat Defense.
- Configure dynamic routing on Cisco Secure Firewall Threat Defense.
- Configure advanced NAT on Cisco Secure Firewall Threat Defense.
- Configure SSL policy on Cisco Secure Firewall Threat Defense.
- Deploy remote VPN access on Cisco Secure Firewall Threat Defense.
- Deploy identity-based policies on Cisco Secure Firewall Threat Defense.
- Deploy a site-to-site VPN on Cisco Secure Firewall Threat Defense.
- Configure Snort rules and network analysis policies.
- Describe advanced event management on Cisco Secure Firewall Threat Defense.
- Describe Cisco Secure Firewall Threat Defense integrations.
- Troubleshoot advanced traffic flows on Cisco Secure Firewall Threat Defense.
- Automate Cisco Secure Firewall Threat Defense.
- Migrate to Cisco Secure Firewall Threat Defense

2 Official practical work

- Deploy advanced connection parameters.
- Configure dynamic routing.
- Configure SSL policy.
- Configure remote access VPN.
- Configure site-to-site VPN.
- Customize IPS and NAP policies.
- Configure Cisco Secure Firewall threat defense integrations.
- Troubleshooting Cisco Secure Firewall Threat Defense.
- Migrate Cisco Secure Firewall ASA configuration.

Options

Certification : 330 € HT

This course prepares you for the 300-710 Securing Networks with Cisco Firepower (SNCF) exam. On successful completion, you will be certified as a "Cisco Certified Specialist - Network Security Firepower" and meet the requirements of the concentration exam for certification as a "Cisco Certified Networking Professional (CCNP) Security".
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.

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.