

Advanced Techniques for Cisco Firewall Threat Defense and Intrusion Prevention

Durée: 5 Jours **Réf de cours: SFWIPA** **Version: 1.0** **Méthodes d'apprentissage: Classe à distance**

Résumé:

The Securing Data Center Networks and VPNs with Cisco Secure Firewall Threat Defense training shows you how to deploy Cisco Secure Firewall Threat Defense system and its features as a data center network firewall or as an Internet Edge firewall with VPN support.

The Securing Data Center Networks and VPNs with Cisco Secure Firewall Threat Defense training shows you how to deploy and configure Cisco Secure Firewall Threat Defense system and its features as a data center network firewall or as an Internet Edge firewall with Virtual Private Network (VPN) support. You will learn how to configure identity-based policies, Secure Sockets Layer (SSL) decryption, remote-access VPN, and site-to-site VPN before moving on to advanced Intrusion Prevention System (IPS) configuration and event management, integrations with other systems, and advanced troubleshooting. You will also learn how to automate configuration and operations of Cisco Secure Firewall Threat Defense system using programmability and Application Programming Interfaces (APIs) and how to migrate configuration from Cisco Secure Firewall Adaptive Security Appliances (ASA).

This training prepares you for the 300-710 Securing Networks with Cisco Firepower (SNCF) exam. If passed, you earn the Cisco Certified Specialist – Network Security Firepower certification and satisfy the concentration exam requirement for the Cisco Certified Networking Professional (CCNP) Security certification. This training also earns you 40 Continuing Education (CE) credits toward recertification.

Virtual and Classroom learning - V&C Select™

V&C Select™ is a simple concept and a flexible approach to delivery. You can 'select' a course from our public schedule and attend in person or as a virtual delegate. Virtual delegates do not travel to this course, we will send you all the information you need before the start of the course and you can test the logins.

Public visé:

System Installers System Integrators System Administrators Network Administrators Solutions Designers

Objectifs pédagogiques:

- Describe Cisco Secure Firewall Threat Defense
- Describe advanced deployment options on Cisco Secure Firewall Threat Defense
- Describe advanced device settings for Cisco Secure Firewall Threat Defense device
- Configure dynamic routing on Cisco Secure Firewall Threat Defense
- Configure advanced network address translation on Cisco Secure Firewall Threat Defense
- Configure SSL decryption policy on Cisco Secure Firewall Threat Defense
- Deploy Remote Access VPN on Cisco Secure Firewall Threat Defense
- Deploy identity-based policies on Cisco Secure Firewall Threat Defense
- Deploy site-to-site IPsec-based VPN on Cisco Secure Firewall Threat Defense
- Deploy advanced access control settings on Cisco Secure Firewall Threat Defense
- Describe advanced event management on Cisco Secure Firewall Threat Defense
- Describe available integrations with Cisco Secure Firewall Threat Defense
- Troubleshoot traffic flow using advanced options on Cisco Secure Firewall Threat Defense
- Describe benefits of automating configuration and operations of Cisco Secure Firewall Threat Defense
- Describe configuration migration to Cisco Secure Firewall Threat Defense

Pré-requis:

Attendees should meet the following prerequisites:

- Knowledge of Transmission Control Protocol/Internet Protocol (TCP/IP)
- Basic knowledge of routing protocols
- Familiarity with the content explained in the Securing Internet Edge with Cisco Secure Firewall Threat Defense training
- These skills can be found in the following Cisco Courses:
 - Implementing and Administering Cisco Solutions v2.0
 - Securing Internet Edge with Cisco Secure Firewall Threat Defense 1.0
- SFWIPF - Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention

Test et certification

Recommended as preparation for the following exam:

- 300-710 - Securing Networks with Cisco Firewall Exam
Exam topics are currently spread over two courses SSNGFW and SSFIPS, these are being replaced with SFWIPF and SFWIPA
- Cisco Certified Specialist Network Security Firepower

Contenu:

This training will help you:

- Attain advanced knowledge of Cisco Secure Firewall Threat Defense technology
- Gain competency and skills required to implement and manage a Cisco Secure Firewall Threat Defense system regardless of platform
- Learn detailed information on policy management, traffic flow through the system, and the system architecture
- Deploy and manage many of the advanced features available in the Cisco Secure Firewall Threat Defense system
- Gain knowledge for protocols, solutions, and designs to acquire professional-level and expert-level data center roles
- Earn 40 CE credits toward recertification

Course Outlines:

- Introducing Cisco Secure Firewall Threat Defense
- Describing Advanced Deployment Options on Cisco Secure Firewall Threat Defense
- Configuring Advanced Device Settings on Cisco Secure Firewall Threat Defense
- Configuring Dynamic Routing on Cisco Secure Firewall Threat Defense
- Configuring Advanced NAT on Cisco Secure Firewall Threat Defense
- Configuring SSL Policy on Cisco Secure Firewall Threat Defense
- Deploying Remote Access VPN on Cisco Secure Firewall Threat Defense
- Deploying Identity-Based Policies on Cisco Secure Firewall Threat Defense
- Deploying Site-to-Site VPN on Cisco Secure Firewall Threat Defense
- Configuring Snort Rules and Network Analysis Policies
- Describing Advanced Event Management Cisco Secure Firewall Threat Defense
- Describing Integrations on Cisco Secure Firewall Threat Defense
- Troubleshooting Advanced Traffic Flow on Cisco Secure Firewall Threat Defense
- Automating Cisco Secure Firewall Threat Defense
- Migrating to Cisco Secure Firewall Threat Defense
- Deploy Advanced Connection Settings
- 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
- Troubleshoot Cisco Secure Firewall Threat Defense
- Migrate Configuration from Cisco Secure Firewall ASA

Labs Outlines:

- Introducing Cisco Secure Firewall Threat Defense
- Describing Advanced Deployment Options on Cisco Secure Firewall Threat Defense
- Configuring Advanced Device Settings on Cisco Secure Firewall Threat Defense
- Configuring Dynamic Routing on Cisco Secure Firewall Threat Defense
- Configuring Advanced NAT on Cisco Secure Firewall Threat Defense
- Configuring SSL Policy on Cisco Secure Firewall Threat Defense
- Deploying Remote Access VPN on Cisco Secure Firewall Threat Defense
- Deploying Identity-Based Policies on Cisco Secure Firewall Threat Defense
- Deploying Site-to-Site VPN on Cisco Secure Firewall Threat Defense
- Configuring Snort Rules and Network Analysis Policies
- Describing Advanced Event Management Cisco Secure Firewall Threat Defense
- Describing Integrations on Cisco Secure Firewall Threat Defense
- Troubleshooting Advanced Traffic Flow on Cisco Secure Firewall Threat Defense
- Automating Cisco Secure Firewall Threat Defense
- Migrating to Cisco Secure Firewall Threat Defense
- Deploy Advanced Connection Settings
- 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
- Troubleshoot Cisco Secure Firewall Threat Defense
- Migrate Configuration from Cisco Secure Firewall ASA

Autres moyens pédagogiques et de suivi:

- Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
- Suivi d'exécution : Une feuille d'embarquement par demi-journée de présence est signée par tous les participants et le formateur.
- En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

- Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
- Votre place sera confirmée à la réception d'un devis ou "booking form" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
- Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non