Formation : Certified Stormshield Network Administrator (NT-CSNA)

Découvrez les fonctionnalités et la procédure d'installation des produits

Cours pratique - 3j - 21h00 - Réf. CNG
Prix : 2600 € H.T.

4,7 / 5

BEST

Cette formation a pour but de présenter la gamme et les fonctionnalités de base du produit Stormshield Network Security. Reconnue par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) comme ayant une forte valeur d'usage dans un cadre professionnel, cette certification est labellisée SecNumedu - Formation continue.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Prendre en main un firewall SNS et connaître son fonctionnement
- Configurer un firewall dans un réseau
- Définir et mettre en œuvre des politiques de filtrage et de routage
- Configurer un contrôle d'accès aux sites web en http et https (proxy)
- Configurer des politiques d'authentification
- Mettre en place différents types de réseaux privés virtuels (VPN IPSec et VPN SSL)

Public concerné

Responsables informatique, administrateurs réseaux, tous techniciens informatique.

Prérequis

Bonnes connaissances TCP/IP. Avoir suivi une formation réseau préalable est un plus.

PARTICIPANTS

Responsables informatique, administrateurs réseaux, tous techniciens informatique.

PRÉREQUIS

Bonnes connaissances TCP/IP. Avoir suivi une formation réseau préalable est un plus.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.
Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.
Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation...
À l'issue de chaque formation, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur.
Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

Certification

La certification consiste en un examen effectué en ligne (1h30, 70 questions). Le score minimum de certification est de 70%. L'examen est ouvert automatiquement le jour suivant la fin de la formation pour une durée de trois semaines sur la plateforme https://institute.stormshield.eu. En cas d'échec ou d'impossibilité de passer l'examen dans ce créneau, un deuxième et dernier passage d'examen est ouvert automatiquement dans la foulée pour une durée d'une semaine. Certification SecNumedu.
Comment passer votre examen ?

Méthodes et moyens pédagogiques

Méthodes pédagogiques

La formation est délivrée soit en présentiel (en face à face pédagogique et en salle), soit en distanciel (présence à distance du formateur grâce à un système de visio et utilisation de la plateforme CyberRange d'Airbus). La formation alterne cours théorique et travaux pratiques. Les participants reçoivent un support de cours composé du cours, des travaux pratiques (Labs) et de leurs corrections. Afin de pouvoir mettre en pratique les éléments du cours, les participants ont à leur disposition un environnement technique complet. Afin de maintenir l'expertise du participant, toutes les mises à jour du support de cours sont accessibles au format PDF durant 3 ans sur notre plateforme https://institute.stormshield.eu. Le participant trouvera également sur cette plateforme un environnement virtuel lui permettant de manipuler le produit et rejouer les Labs en toute autonomie.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

1 Introduction

- Présentation des participants (tour de table).
- Cursus des formations et certifications.
- Présentation de l'entreprise et des produits Stormshield.

2 Prise en main du firewall

- Enregistrement sur l'espace client et accès à la base de connaissances.
- Initialisation du boîtier et présentation de l'interface d'administration.
- Configuration système et droits d'administration.
- Installation de la licence et mise à jour de la version du système.
- Sauvegarde et restauration d'une configuration.

3 Traces et supervisions

- Présentation des catégories de traces.
- Supervision et graphiques d'historiques.

4 Les objets

- Notion d'objet et types d'objets utilisables.
- Objets réseau et routeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

5 Configuration réseau

- Modes de configuration d'un boîtier dans un réseau.
- Types d'interfaces (Ethernet, modem, bridge, VLAN, GRETAP).
- Types de routage et priorités.

6 Translation d'adresses (NAT)

- Translation sur flux sortant (déguisement).
- Translation sur flux entrant (redirection).
- Translation bidirectionnelle (translation un pour un).

7 Filtrage

- Généralités sur le filtrage et notion de suivi de connexion (stateful).
- Présentation détaillée des paramètres d'une règle de filtrage.
- Ordonnancement des règles de filtrage et de translation.

8 Protection applicative

- Mise en place du filtrage URL en http et https.
- Configuration de l'analyse antivirale et de l'analyse par détonation Breach Fighter.
- Module de prévention d'intrusion et profils d'inspection de sécurité.

9 Utilisateurs et authentification

- Configuration des annuaires.
- Présentation des différentes méthodes d'authentification (LDAP, Kerberos, Radius, Certificat SSL, SPNEGO, SSO).
- Enrôlement d'utilisateurs.
- Mise en place d'une authentification explicite via portail captif.

10 Les réseaux privés virtuels

- Concepts et généralités VPN IPSec (IKEv1 IKEv2).
- Site à site avec clé prépartagée.
- Virtual Tunneling Interface.

11 VPN SSL

- Principe de fonctionnement.
- Configuration.

Dates et lieux

CLASSE À DISTANCE
2026 : 18 mai, 15 juil., 9 sep., 2 déc.

PARIS LA DÉFENSE
2026 : 11 mai, 8 juil., 2 sep., 25 nov.