Formation : Palo Alto Networks - Firewall 11.1 Essentials : Configuration and Management (EDU-210)

Cours officiel, préparation aux examens Palo Alto Networks

Cours pratique - 5j - 35h00 - Réf. PA1
Prix : 4070 € H.T.

4,7 / 5

Avec cette formation, vous saurez configurer et gérer les fonctionnalités clés des pare-feux nouvelle génération Palo Alto Networks. Vous apprendrez à mettre en place des règles de sécurité et de NAT pour autoriser le trafic légitime entre les zones, à appliquer des stratégies de prévention des menaces pour bloquer les IP, domaines et URLs malveillants, et à surveiller le réseau via l'interface web et les rapports intégrés.

Objectifs pédagogiques

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

- Configurer et gérer un pare-feu Palo Alto Networks
- Appliquer des règles de sécurité adaptées au trafic réseau
- Mettre en place des stratégies de prévention des menaces
- Surveiller et analyser le trafic via l'interface et les rapports

Public concerné

Ingénieurs sécurité, administrateurs, analystes, spécialistes des opérations de sécurité et équipes de support.

Prérequis

Connaître les bases du réseau (routage, commutation, adressage IP) et de la sécurité, une expérience avec des technologies comme IPS, proxy ou filtrage de contenu est un plus.

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

PARTICIPANTS

Ingénieurs sécurité, administrateurs, analystes, spécialistes des opérations de sécurité et équipes de support.

PRÉREQUIS

Connaître les bases du réseau (routage, commutation, adressage IP) et de la sécurité, une expérience avec des technologies comme IPS, proxy ou filtrage de contenu 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.

Méthodes et moyens pédagogiques

Méthodes pédagogiques

Animation de la formation en français. Support de cours officiel au format numérique et en anglais. Bonne compréhension de l'anglais à l'écrit.

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. **Module 1 : Portefeuille et architecture de Palo Alto Networks**
2. **Module 2 : Configuration des paramètres initiaux du pare-feu**
3. **Module 3 : Gestion des configurations du pare-feu**
4. **Module 4 : Gestion des comptes administrateurs du pare-feu**
5. **Module 5 : Connexion du pare-feu aux réseaux via zones de sécurité**
6. **Module 6 : Création et gestion des règles de la politique de sécurité**
7. **Module 7 : Création et gestion des règles de la politique NAT**
8. **Module 8 : Contrôle de l'utilisation des applications avec APP-ID**
9. **Module 9 : Blocage des menaces connues à l'aide de profils de sécurité**
10. **Module 10 : Blocage du trafic web inapproprié avec le filtrage des URL**
11. **Module 11 : Blocage des menaces inconnues avec WildFire**
12. **Module 12 : Contrôle de l'accès aux ressources du réseau avec user-ID**
13. **Module 13 : Déchiffrer pour bloquer les menaces chiffrées**
14. **Module 14 : Exploiter les journaux et rapports pour trouver des infos clés**
15. **Module 15 : Prochaines étapes de votre formation et de votre certification**

MOYENS PÉDAGOGIQUES ET TECHNIQUES

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

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.

16 **Annexe A : Sécuriser les points de terminaison avec Global Protect**

17 **Annexe B : Assurer la redondance du pare-feu avec la haute disponibilité**

18 **Annexe C : Connecter des sites distants à l'aide des VPN**

19 **Annexe D : Bloquer les attaques courantes avec la protection de zone**

Options

Certification : 260 € HT

Cette formation est recommandée dans le parcours de préparation aux examens suivants : Network Security Professional, Next-Generation Firewall Engineer, Network Security Analyst.
Comment passer votre examen ?

L'option de certification se présente sous la forme d'un voucher ou d'une convocation qui vous permettra de passer l'examen à l'issue de la formation.

Dates et lieux

CLASSE À DISTANCE
2026 : 23 mars, 1 juin, 27 juil., 28 sep., 23 nov.

PARIS LA DÉFENSE
2026 : 23 mars, 1 juin, 28 sep., 23 nov.