

PALO ALTO NETWORKS FIREWALL 11.X ESSENTIELS : CONFIGURATION ET MANAGEMENT

— Public	Ingénieurs et administrateurs réseau et sécurité, aux analystes sécurité, administrateurs systèmes, ainsi qu'aux personnes en charge du support technique.
— Durée	5 jours - 35 heures
— Pré-requis	Les participants doivent être familiers avec les concepts basiques de la sécurité et des réseaux, incluant routage, switching et adresses IP. Une expérience sur des technologies de sécurité (IPS, proxy, filtrage de contenus) est un plus.
— Objectifs	Configurer et gérer les fonctionnalités essentielles des firewalls Palo Alto Networks de nouvelles générations Configurer et gérer des règles de sécurité et de NAT pour la gestion des flux autorisés Configurer et gérer les profils de gestion des menaces afin de bloquer les trafics provenant des adresses, domaines et URLs connues et inconnues Monitorer le trafic réseau en utilisant l'interfaces web et les rapports intégrés
— Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
— Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
— Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
— Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
— Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

CONTENU

- Palo Alto Networks portfolio et architecture
- Configuration initiale du Firewall
- Gérer les configurations sur le Firewall
- Gérer les comptes d'administration du Firewall
- Connection du Firewall aux réseaux de production avec zones de sécurité
- Création et gestion des règles de sécurité
- Création et gestion des règles de NAT
- Contrôle des applications avec App-ID
- Blocages des menaces connues en utilisant les profils de sécurité
- Blocage du trafic web non approprié avec le filtrage des URLs
- Bloquer les menaces inconnues avec Wildfire
- Contrôler l'accès aux ressources réseaux avec la reconnaissance utilisateurs (User-ID)
- Utiliser le déchiffrement afin de bloquer les menaces sur un trafic chiffré
- Repérer les informations importantes via les logs et les rapports
- Discussion sur les autres formations et les certifications

ANNEXE

- Annexe A - Sécuriser les postes de travail avec Global Protect
- Annexe B - Apporter de la redondance au Firewall avec la haute disponibilité
- Annexe C - Connecter des sites distants via des VPN site à site
- Annexe D - Configuration de l'agent Windows User-ID

NOUS CONTACTER

Siège social

16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Téléphone

04 76 23 20 50 - 06 81 73 19 35

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !



ACF Audit Conseil Formation



@ACF_Formation

Dernière mise à jour : 31/07/2026

PROFIL Formateur : Les formateurs sont recrutés selon plusieurs critères :
Expérience, pédagogie, dynamisme et prévoyance.