

# Palo Alto - Troubleshooting

## Publics

Ingénieurs sécurité, Administrateurs sécurité, Analystes en sécurité, Ingénieurs réseaux et membre d'une équipe de support.

## Pré-requis

Les participants devront avoir suivi les formations Palo Alto Networks Firewall 10.1: Configuration & Management (PAN-EDU-210), Palo Alto Networks Firewall 10.1 : Improving Security Posture and Hardening PAN-OS Firewalls (PAN-EDU-214) ou avoir une expérience pratique correspondante.

Les stagiaires devront être familiers avec les fondamentaux des concepts réseaux (routage, switching et adressage IP. Ils devront également avoir au moins 6 mois d'expérience professionnelle sur les firewalls Palo Alto Networks

## Objectifs pédagogiques

Être capable de :

- Investiguer les problèmes de connexion réseau en utilisant les outils et la CLI
- Suivre des procédures de troubleshooting éprouvées
- Analyse avancée des logs pour résoudre des scénarios variés du quotidien
- Mettre en pratique ces méthodes dans des labs. (exercices pratiques delab basés sur des scenarios)

## Moyens pédagogiques et techniques

Explications théoriques et exercices pratiques pour mise en situation rapide

1 vidéoprojecteur par salle

1 ordinateur par stagiaire

1 support de cours par stagiaire

## Évaluation et documents fournis

- Document d'évaluation de satisfaction
- Attestation de présence
- Exercices pratiques de validation des acquis sous contrôle du formateur

**Mise à jour :** Octobre 2024

**Tarifs Inter :** 890€ HT/jour/pers.

**Tarifs Intra / sur mesure :** nous consulter

**Délais :** nous consulter

**Moyens d'encadrement:**

formateur spécialiste du domaine

**Référence :** SRS



**Lieu :** • Centre de formation Konica Minolta  
• Site client (nous consulter)



**Durée totale :** 3 jours (21 heures)



**Nombre de participants :** 4 maximum

## Programme

### Module 1

- Outils et ressources

### Module 2

- Gestion des sessions

### Module 3

- Capture de Paquets

### Module 4

- Analyse bas niveau – Paquet

### Module 5

- Gestion des sessions à destination du Firewall

### Module 6

- Gestion des sessions traversant le Firewall

### Module 7

- Services internes

### Module 8

- Gestion des certificats et déchiffrement SSL

### Module 9

- Identification des Users User- ID

### Module 10

- VPN Nomade, GlobalProtect

### Module 11

- Ouverture des tickets, escalade et RMA

### Module 12

- Et après ...

- Annexe : Introduction aux lignes de commandes