Organisme de formation référencé Datadock

CJFV - Configuring Juniper Networks firewall IPSEC VPN

Objectifs de la formation :

Cette formation est le premier du curriculum ScreenOS. Il cible les connaissances sur les configurations des produits Juniper Firewall et VPN, dans des situations variées, incluant l'accès administratif de base, le routage, les politiques Firewall, les préventions d'attaques.

Moyens pédagogiques :
Formation présentielle, exposés, cas pratiques, synthèse, assistance post-formation. 1 poste par stagiaire, vidéoprojecteur, support de cours fourni à chaque stagiaire.

Pré-requis :

Connaissance des terminologies réseaux et sécurité, adressages, TCP/IP, routage et concept d'Internet.

Moyens et méthodes pédagogiques :

Les prestations de formation sont assurées par des formateurs professionnels qui utilisent des moyens pédagogiques adaptés.

En amont de la formation :
Si besoin, nous auditons les stagiaires afin de constituer des groupes homogènes
Dans le cadre de session intra entreprise, les formateurs adaptent les programmes et animent des formations spécifiques sur site afin de répondre à vos besoins spécifiques.
Pour un bon suivi du stage, le stagiaire dispose d'un ou plusieurs supports de cours.

Après le stage :
Le stagiaire dispose d'une évaluation globale du stage.
Les formateurs partagent leurs expériences dans un but d'amélioration continue.

Modalités d'évaluation :

Evaluation à chaud par le biais de travaux pratiques.

Moyens techniques :

Salle(s) de cours équipée(s) des moyens audiovisuels avec le matériel adapté à la formation (si besoin, ordinateur par stagiaire).

Public :

Ingénieur sécurité, administrateur sécurité, ingénieur réseaux.

Durée :	Référence :	Type de formation :
3 jours	PRO-CJF-0550	Formation qualifiante

Programme de la formation

1. ScreenOS : Concepts, terminologie et plateforme

Pré-requis d'un équipement de sécurité Architecture ScreenOS
Les plateformes Juniper

2. Configuration initiale

Composants
Effectuer la configuration initiale Vérification

3. Gestion du boîtier

Gestion et récupération

4. Opération Niveau 3

Besoin du routage Configuration du niveau 3 Vérification
Interface de Loopback Interface-based NAT

5. Configuration d'une politique (Basique)

Fonctionnalités et configuration Problèmes courants
Politique globale
Vérification du fonctionnement des politiques

6. Politiques : Options

Aperçu Logging Counting Scheduling
Authentification utilisateur

7. Translation d'adresses

Scénario NAT src NAT dst Adresse VIP Adresse MIP

8. Mode transparent

Description Configuration
Vérification du fonctionnement

9. Concepts VPN

Concepts et terminologie Sécurité IP

10. VPN : Policy-Based

Configuration
Vérification du fonctionnement

11. VPN : Route-Based

Concepts et terminologie Configuration
Vérification du fonctionnement