+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 18/12/2025

S'inscrire

Formation Certification JNCIS-SEC

3 jours (21 heures)

Présentation

JNCIS-SEC est une certification de niveau Specialist entièrement dédiée à la maîtrise de la sécurité réseau sur les pare-feu Juniper SRX. Basée sur un moteur de sécurité flow-based performant, la plateforme Juniper Security permet de protéger les infrastructures d'entreprise grâce à des politiques avancées, du NAT, des VPN IPsec et des services de contrôle applicatif.

Notre formation JNCIS-SEC vous permettra de comprendre en profondeur l'architecture SRX, de construire des politiques de sécurité efficaces, de déployer des scénarios de NAT complexes, de mettre en œuvre des VPN IPsec et d'exploiter les fonctionnalités AppSecure.

Vous apprendrez également à diagnostiquer les incidents, à analyser les logs et à mettre en place un environnement haute disponibilité adapté à la production.

Une partie de la formation est spécifiquement consacrée à la préparation de l'examen JNCIS-SEC (JN0-335) : revue détaillée du blueprint, conseils de révision, bonnes pratiques et exercices ciblés.

À l'issue de cette formation, vous serez en mesure d'administrer au quotidien des pare-feu Juniper SRX et d'aborder la certification JNCIS-SEC avec confiance.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Comprendre l'architecture de sécurité des pare-feu Juniper SRX.
- Configurer et optimiser des politiques de sécurité avancées.
- Mettre en œuvre et dépanner le NAT et les VPN IPsec.

- Utiliser AppSecure pour la visibilité et le contrôle applicatif.
- Déployer un environnement SRX en haute disponibilité.
- Se préparer efficacement à l’examen JNCIS-SEC (JN0-335).

Public visé

- Ingénieurs sécurité
- Administrateurs réseau
- Techniciens sécurité
- Professionnels IT préparant la certification JNCIS-SEC

Pré-requis

- Bonnes connaissances de base en TCP/IP, routage et firewalling
- Niveau équivalent à JNCIA
- Pratique préalable sur un réseau d’entreprise

Programme de formation JNCIS-SEC

[Jour 1 - Matin]

Fondamentaux de la sécurité Juniper et architecture SRX

- Présentation de la gamme SRX et positionnement dans l’architecture de sécurité
- Comprendre le moteur flow-based et le traitement des paquets
- Zones de sécurité, interfaces et modèle de segmentation
- Objets de configuration : Address Book, applications, services
- Principes de base de la stratégie de sécurité Juniper
- Atelier pratique : Prise en main d’un SRX et exploration du mode flow.

[Jour 1 - Après-midi]

Politiques de sécurité : création, logique et bonnes pratiques

- Structure d’une Security Policy et ordre d’évaluation
- Policies basées sur l’adresse, l’application et l’utilisateur
- Gestion du logging et suivi des décisions de sécurité
- Organisation, lisibilité et optimisation des règles
- Premiers réflexes de troubleshooting des policies
- Atelier pratique : Création et test d’un jeu complet de politiques.

NAT : source, destination, static et scénarios avancés

- Concepts de source NAT, destination NAT et static NAT
- Traduction de ports, port-overloading et comportements spécifiques
- Interaction entre NAT et Security Policies
- Cas d’usage typiques : sortie Internet, DMZ, accès publié
- Outils de diagnostic : traces, tables et sessions
- Atelier pratique : Mise en place d’un scénario NAT complet et analyse des flux.

[Jour 2 - Matin]

VPN IPsec site-à-site et accès distant

- Rappels sur les concepts IPsec : IKE, Phase 1 et Phase 2
- Création et paramétrage d’un VPN site-à-site sur SRX
- Gestion des propositions, profils et stratégies de chiffrement
- Topologies courantes : site-à-site, hub-and-spoke, multi-site
- Méthodes de troubleshooting des VPN IPsec
- Atelier pratique : Déploiement et test d’un VPN IPsec entre deux SRX.

[Jour 2 - Après-midi]

Routage, zones avancées et services de sécurité

- Intégration du routage statique et dynamique avec les SRX
- Utilisation avancée des zones et de host-inbound-traffic
- Options de protection screen et durcissement L3/L4
- Gestion des services critiques
- Positionnement des SRX dans l’architecture globale du réseau
- Atelier pratique : Configuration d’un routage sécurisé multi-zones.

AppSecure : visibilité et contrôle des applications

- Composants AppSecure : AppID, AppFW, AppTrack
- Création de politiques basées sur les applications
- Utilisation d’AppTrack pour la visibilité du trafic applicatif
- Analyse et contrôle des applications critiques ou non autorisées
- Intégration AppSecure avec les politiques de sécurité existantes
- Atelier pratique : Mise en œuvre d’AppTrack et AppFW sur un cas réel.

[Jour 3 - Matin]

Haute disponibilité et redondance SRX

- Principes du chassis cluster sur SRX
- Modes actifs/passifs et scénarios de bascule
- Synchronisation des états et des sessions

- Surveillance des liens, interfaces et chemins critiques
- Bonnes pratiques de déploiement HA en production
- Atelier pratique : Configuration d’un cluster SRX et tests de bascule.

[Jour 3 - Après-midi]

Détection, prévention et supervision

- Utilisation des logs, events et journaux de trafic
- Outils de troubleshooting : flow sessions, captures, traceoptions
- Détection des anomalies et attaques courantes
- Intégration avec les outils de supervision ou de SIEM
- Bonnes pratiques d’exploitation quotidienne d’un SRX
- Atelier pratique : Analyse d’incidents et diagnostic avancé.

Préparation à la certification JNCIS-SEC (JN0-335)

- Structure, format et exigences de l’examen JNCIS-SEC
- Revue détaillée des domaines du blueprint officiel
- Pièges fréquents et méthodes pour analyser les questions
- Plan de révision : documentation, labs, ressources Juniper
- Stratégies de gestion du temps et de validation des réponses
- Atelier pratique : Passage de l'examen blanc + correction.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des

séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.