Sécurité Junos - Juniper

Durée: 5 Jours **Réf de cours: JSEC** **Version: 17.a**

Résumé:

Cette formation permet aux participants d'acquérir les compétences et connaissances nécessaires pour configurer, utiliser et mettre en œuvre les SRX Services Gateways dans un environnement réseau typique. Les sujets clés abordés lors de la formation incluent : les zones de sécurité, les stratégies sécurité, NAT (Network Address Translation), IPSec, VPNs et les clusters de châssis.
Au travers de démonstrations et d'exercices pratiques, les participants acquerront l'expérience dans la configuration du système d'exploitation Junos et la surveillance du fonctionnement des périphériques.
Cette formation s'adresse aux ingénieurs réseaux, aux administrateurs et aux membres du support.
Mise à jour : 23.05.2023

Public visé:

Cette formation s'adresse aux ingénieurs réseaux, aux administrateurs et au personnel du support.

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Décrire le routage et la sécurité traditionnel
- Présenter une vue d'ensemble des périphériques SRX Series Services Gateway et de l'architecture logicielle de Junos OS.
- Décrire le flux de paquets logiques et la création de sessions améliorées par les périphériques SRX Serirs Services Gateway
- Décrire, configurer, surveiller les zones et les stratégies de sécurité
- Dépanner les zones de sécurité et les stratégies
- Décrire, configurer et surveiller NAT implémenté sur les plateformes de sécurité Junos
- Expliquer les objectifs et mécanismes de IPSec (IP Security) et des VPNs (Virtual Private Networks)
- Mettre en oeuvre et surveiller IPsec VPNs route-based, les VPNs Hub-and-Spoke, les groupes VPNs et les ADVPNs
- Dépanner les VPNs IPSec et les clusters de châssis
- Décrire, configurer et surveiller les clusters de cassis

Pré-requis:

Avoir suivi la formation IJOS ou posséder les connaissances équivalentes.

Posséder des connaissances du modèle OSI et de la suite de protocoles TCP/IP.

- IJSEC - Introduction to Junos Security

Test et certification

Cette formation prépare au titre de certification JNCIS*-SEC de niveau intermédiaire, après avoir réussi l'examen JN0-333.
*Juniper Networks Certified Internet Specialist

Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

La formation suivante est recommandée à tous les candidats à la certification Juniper JNCIP-SEC ou les professionnels qui souhaitent approfondir leur expertise en sécurité dans un environnement réseau Juniper :

- Sécurité avancée Junos (AJSEC)
- AJSEC - Sécurité avancée Junos - Juniper

Contenu:

Introduction à la sécurité Junos

- Routage traditionnel et sécurité
- Vue d'ensemble de l'architecture des périphériques de sécurité Junos
- Flux des paquets logiques via les périphériques de sécurité Junos
- Vue d'ensemble de J-Web

Zones et options

- Définition des zones
- Configuration des zones
- Surveiller les zones de sécurité
- Configurer les options SCREEN
- Etudes de cas

Stratégies de Sécurité

- Vue d'ensemble des stratégies de sécurité
- Composants des stratégies
- Configurer les stratégies de sécurité dans J-Web
- Etudes de cas

Stratégie de sécurité avancée

- Gérer les sessions
- Junos ALGs
- Planifier les stratégies
- Logging
- Stratégie de sécurité avancée

Dépannage des Zones et Stratégies

- Dépanner les périphériques Junos
- Outils de dépannage
- Zones et stratégies de dépannage
- Etudes de cas

Network Translation Address

- Vue d'ensemble de NAT
- NAT Source
- NAT Destination
- NAT statique
- ARP Proxy
- Configurer NAT dans Security Director

NAT avancé

- Persistence NAT
- Doctoring DNS
- IPv6 avec NAT
- Scénarios NAT avancés
- Dépanner NAT

Concepts VPN IPSec

- Types de VPN
- Prérequis pour un VPN sécurisé
- Etablir un tunnel IPSec
- Process de trafic IPSec

Mettre en œuvre VPN IPSec

- Configuration VPN IPSec
- Etude de cas
- IDs Proxy et sélecteur de trafic
- Surveiller les VPNs IPSec

VPNs Hub-and-Spoke

- Vue d'ensemble de VPN Hub-and-Spoke
- Configuration et surveillance de Hub-and-Spoke

Groupes VPNs

- Vue d'ensemble des groupes VPN
- Configurer et surveiller les groupes VPN

PKI et ADVPNs

- Vue d'ensemble de l'infrastructure à clé publique
- Configurer les PKI
- Vue d'ensemble de ADVPN
- Configurer et surveiller de ADVPN

IPsec Avancé

- NAT avec IPsec
- Classe de Service avec IPsec
- Meilleures pratiques
- Le routage OSPF over IPsec
- IPsec avec des adresse Overlapping
- IPsec avec les adresses dynamiques Gateway IP

Dépannage IPSec

- Vue d'ensemble du dépannage IPSec
- Dépanner IKE Phase 1 et 2
- Logging IPSec
- Etude de cas

Concepts de cluster de Châssis

- Vue d'ensemble du cluster de châssis
- Composants du cluster de châssis
- Fonctionnement du cluster de châssis

Mise en œuvre de cluster de châssis

- Configurer le cluster de châssis
- Options avancées du cluster de châssis

Dépannage des clusters de châssis

- Dépanner les cluster de châssis
- Etudes de cas

Appendice A : Matériel t interface SRX Series

- Vue d'ensemble de la plateforme SRX
- Vue d'ensemble de la plateforme SRX High-End
- Flux du trafic SRX et distribution
- Interfaces SRX

Appendice B : SRX virtuel

- Vue d'ensemble de la virtualisation
- Virtualisation réseau et SDN
- Vue d'ensemble de virtuel SRX
- Scénarios de déploiement
- Intégration avec AWS

Méthodes pédagogiques :

Support de cours officiel en anglais remis aux participants

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• Modalités d'évaluation : le participant est invité à s'auto-évaluer par rapport aux objectifs énoncés.
• Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

•Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
•Votre place sera confirmée à la réception d'un devis ou ""booking form"" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
•Attention, si vous utilisez votre Compte Personnel de Formation pour financer votre inscription, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés.