Sécurité avancée Junos - Juniper

Formation Informatique / Réseaux et Sécurité / Juniper Networks

Cette formation AJSEC permet d'acquérir les compétences et connaissances nécessaires pour développer ses compétences sur la mise en oeuvre et la surveillance de solutions Juniper dédiées : déploiements IPsec, virtualisation, haute-disponibilité, déploiements Network Address Translation (NAT), et sécurité sur la couche 2 avec SRX Series Services Gateways.
Un lab clôture chaque module pour mettre en oeuvre le concept ou la fonctionnalité abordée

OBJECTIFS

- Comprendre les concepts fondamentaux liés aux technologies de sécurité Junos
- Identifier les diverses fonctions sécuritaires supportées par l'OS Junos
- Implémenter les caractéristiques de la suite AppSecure
- Configurer les signatures d'application personnalisées
- Décrire la sécurité Junos traitée sur la couche 2 versus la couche 3
- Implémenter les caractéristiques de sécurité de niveau 2 en mode transparent
- Comprendre LSYS (logical System)
- Implémenter les carnets d'adresses avec l'adressage dynamique
- Concevoir les règles de sécurité en utilisant ALGs, les applications personnalisées, et l'adressage dynamique pour différents scénarios
- Utiliser les outils de Junos debug afin d'analyser les flux de trafic et identifier les modèles et problèmes de processus
- Mettre en œuvre les instances de routage virtuel
- Décrire et configurer le partage de route entre des instances de routage utilisant des logical tunnel interfaces
- Comprendre et mettre en œuvre un NAT (statique, source/destination, dual) au sein d'environnements LAN complexes
- Décrire et implémenter les variantes de Persistent NAT
- Décrire et implémenter la solution Carrier Grade NAT (CGN) pour le NAT IPv6 (NAT 64, NAT46 et DS-Lite)
- Démontrer la compréhension de DNS Doctoring
- Différencier et configurer la sécurité IP standard point-à-point (IPsec), les tunnels VPN, les hub-and-spoke VPNs, les VPNs dynamiques et groupes VPNs
- Décrire les interactions entre NAT et les politiques de sécurité
- Mettre en oeuvre OSPF sur des tunnels IPsec et utiliser la Generic Routing Encapsulation (GRE) pour interconnecter des pare-feux
- Implémenter les tunnels IPSec en utilisant les routeurs virtuels
- Contrôler les opérations des diverses implémentations IPsec VPN
- Découvrir la cryptographie à clé publique pour les certificats
- Utiliser les outils Junos pour le dépannage des implémentations de sécurité Junos
- Réaliser un dépannage des problèmes de sécurité Junos commun

PUBLIC

Cette formation s'adresse aux personnes responsables de la mise en œuvre, de la surveillance et du dépannage des composants sécurité Junos.

PRE-REQUIS

Introduction to the Junos Operating System (IJOS)
Junos Routing Essentials (JRE)
Sécurité Junos (JSEC)

PROGRAMME

Présentation du concept AppSecure

AppID
AppTrack
AppFW
AppDoS
AppQoS

Prise en main des paquets de la couche 2 et des fonctionnalités de sécurité

Mode sécurité transparent
Commutateur Ethernet couche 2

Virtualisation

Vue d'ensemble de la virtualisation
Instances de routage
Système logiques

Concepts avancés NAT

Rappels du fonctionnement
NAT: au-delà des entêtes couche 3 & 4

A retenir

Durée : **5 jours** soit 35h.
Réf. **AJSEC**

01 42 93 52 72

Dates des sessions

Paris
18/11/2019 (Promotion)
06/04/2020
23/11/2020

Cette formation est également proposée en formule INTRA-ENTREPRISE.

Inclus dans cette formation

Coaching Après-COURS

Pendant 30 jours, votre formateur sera disponible pour vous aider. CERTyou s'engage dans la réalisation de vos objectifs.

100% SATISFACTION GARANTIE

Votre garantie 100% SATISFACTION

Notre engagement 100% satisfaction vous garantit la plus grande qualité de formation.

DNS Doctoring
IPv6 NAT
Scenarii avancés NAT
SECURITE

Mise en œuvre d'IPsec

Rappels sur les mises en œuvre des VPN standards
Infrastructure à clé publique (PKI)
Hub-and-Spoke VPNs (VPN en étoile)

Technologies IPsec d'entreprise : VPNs de groupes et VPNs dynamiques

Vue d'ensemble des VPN de groupes
Protocole GDOI
Configuration et surveillance des VPN de groupes
Vue d'ensemble des VPN dynamiques
Mettre en œuvre les VPN dynamiques

Etudes de cas des VPN IPsec et Solutions

Routage sur VPNs
IPsec avec les adresses «Overlapping»
Passerelle d'adresses IP dynamiques
Trucs et astuces pour le déploiement de VPN d'entreprise

Dépannage de la sécurité Junos

Méthodologie de dépannage
Outils de dépannage
Identifier les problèmes IPSec
Annexe: Matériel SeriesSRX et interfaces

Horaires, Planning et Déroulement de cette formation

Horaires

- Formation de 9h00 (9h30 le premier jour) à 17h30.
- Deux pauses de 15 minutes le matin et l'après-midi.
- 1 heure de pause déjeuner

DEROULEMENT

- Les horaires de fin de journée sont adaptés en fonction des horaires des trains ou des avions des différents participants.
- Une attestation de suivi de formation vous sera remise en fin de formation.
- Cette formation est organisée pour un maximum de 14 participants.

PROCHAINES FORMATIONS

Réussir la Certification Gestion de Projet PMP du PMI
Réussir la Certification PRINCE2 Foundation
Réussir les Certifications PRINCE2 Foundation et PRINCE2 Practitioner
Réussir la Certification ITIL Foundation
Réussir la Certification Agile certifié SCRUM Master
Réussir les Certifications TOGAF Certified et TOGAF Foundation

Retrouvez cette formation sur notre site :
Sécurité avancée Junos - Juniper