Cycle Junos Juniper : sécurité

Lien : https://innov-systems.com/formation/cycle-junos-juniper-securite

DURÉE	RÉFÉRENCE	CATÉGORIE
8 jours (56h)	**RST160**	**Juniper**

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Implémenter les principaux moyens de sécurisation des systèmes et des réseaux à l'aide de routeurs Firewall Juniper
- Appréhender le rôle des équipements de sécurité dans la protection de l'entreprise
- Acquérir les compétences nécessaires pour sécuriser le réseau d'entreprise avec les solutions de Juniper Networks

POUR QUI ?

- Techniciens et administrateurs systèmes et réseaux

Innov Systems

Programme détaillé

1 / Introduction à la sécurité Junos

- Vue d'ensemble du vocabulaire de la sécurité informatique
- Aperçu du routage traditionnel et ses vulnérabilités
- Sécurité traditionnelle avec pare-feu séparé, NAT/PAT, VPN
- Nouvelle approche : ramasser la DMZ en une seule machine avec le concept SRX
- 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

2 / Zones et options de sécurité

- Définition et principe des zones
- Configurer les zones de sécurité
- Surveiller les zones de sécurité et le trafic

3 / Politiques de Sécurité

- Notion d'une politique
- Définition des composants d'une politique
- Déclenchement et vérification des politiques
- Cas d'utilisation

4 / Dépannage des Zones et Politiques

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

Innov Systems

5 / Authentification Firewall

- Vue d'ensemble de la problématique de l'authentification
- Authentification transversale
- Authentification par portail captif, groupes de clients
- Utilisation de serveurs externes d'authentification

6 / Filtrage propriétaire de risques connus : SCREEN

- Présentation des classes d'attaques et leurs niveaux d'application
- Typologie d'attaque et leurs parades
- Configurer les options SCREEN

7 / Network Address Translation (NAT)

- Vue d’ensemble de NAT
- NAT Source
- NAT Destination
- NAT Statique
- Le Proxy ARP
- Configurer NAT dans Security Director

8 / Introduction aux IPSec VPN, IDS/IPS

- Vue d'ensemble des VPNs et leurs exigences de sécurité
- Présentation de l'architecture d'IPSec
- Configuration VPN IPSec
- Surveillance des VPN IPSec
- Vue d'ensemble de la Prévention et détection d'intrusion (IDS/IPS)

1 / Rappels

- Revue des protocoles et les algorithmes de sécurité

Innov Systems

- Filtrage :
- en mode paquet
- en mode session
- par VLAN
- La sécurité dans la couche 2 (Ethernet)

2 / Politiques de Sécurité et leurs composants

- Présentation des Passerelles d'Applications Intelligentes (ALG)
- Vue d'ensemble d'applications spécifiques
- Gérer les carnets d'adresses pour le filtrage
- Comprendre le fonctionnement des Security Policies

3 / Virtualisation du routage

- Vue d'ensemble de la virtualisation des routeurs
- Instance de routage
- Systèmes logiques
- L'acheminement conditionné par des filtres

4 / NAT avancé

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

5 / Firewall à haute fiabilité (HA)

- Présentation des principes de HA
- Mise en œuvre du cluster de châssis
- Dépannage des clusters de châssis

Innov Systems

6 / Avancés de HA

- IPv6 et le clustering
- Synchronisation
- Graceful Restart

7 / Mise en oeuvre de VPN IPSec

- Configuration VPN IPSec
- Routage OSPF over IPSec
- IPSec avec adresses de chevauchement
- IPSec avec les adresses IP Dynamic Gateway
- Infrastructure à clé publique PKI

8 / VPN en étoile (Hub and Spoke VPNs)

- Vue d’ensemble de VPN Hub and Spok
- Configuration et surveillance de Hub and Spoke
- Configuration de Hub-and-Spoke avec Security Director
- Les groupes VPN
- Vue d’ensemble des groupes VPN
- Configurer et surveiller les groupes VPN
- Implémentation dynamique de VPN

9 / VPN avec solutions

- Routage par-dessus des VPN
- Recouvrement d'espaces d'adressage
- Adresses IP avec passerelles dynamiques
- Bonnes pratiques de déploiement de VPN

Innov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

15 au 24 Fév. 2027	Présentiel - Casablanca
12 au 21 Avr. 2027	Présentiel - Casablanca
07 au 16 Juin 2027	Présentiel - Casablanca
02 au 11 Août 2027	Présentiel - Casablanca
27 Sep. au 06 Oct. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés