EduGroupe
Accompagner pour réussir

PARE-FEUX JUNIPER

Durée : 3 jours (21 heures)

CONNAISSANCES PREALABLES

- Connaissances fondamentales des réseaux TCP/IP.
- Compréhension des protocoles réseau courants (HTTP, HTTPS, DNS, SMTP, SSH).
- Notions de sécurité réseau recommandées.
- Une expérience sur les équipements réseaux ou pare-feux est un plus.

PROFIL DES STAGIAIRES

- Administrateurs réseaux.
- Administrateurs sécurité.
- Ingénieurs systèmes et réseaux.
- Ingénieurs cybersécurité.
- Exploitants d'infrastructures.
- Toute personne souhaitant administrer des pare-feux Juniper SRX.

OBJECTIFS

À l'issue de la formation, les participants seront capables de :

- Comprendre l'architecture de sécurité Juniper SRX.
- Installer et configurer un pare-feu Juniper.
- Administrer les interfaces, zones de sécurité et politiques de filtrage.
- Configurer le routage et la traduction d'adresses (NAT).
- Mettre en œuvre les VPN IPsec.
- Configurer les services de sécurité avancés.
- Superviser et analyser les événements de sécurité.
- Diagnostiquer les incidents réseau et sécurité.
- Assurer l'exploitation quotidienne d'une infrastructure Juniper SRX.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Présentations théoriques.
- Démonstrations techniques.
- Travaux pratiques sur équipements ou machines virtuelles Juniper SRX.
- Études de cas.
- Exercices de configuration.
- Ateliers de dépannage et d'analyse de trafic..

FORMATEUR

- Consultant formateur expert réseaux et cybersécurité disposant d'une expérience significative dans le déploiement et l'administration des solutions Juniper Networks en environnement de production.

METHODE D'EVALUATION DES ACQUIS

- Exercices pratiques.
- Quiz de validation des connaissances.
- Études de cas.
- Atelier fil rouge.
- Évaluation pratique finale.

CONTENU DU COURS

Jour 1 – Découverte de Juniper SRX et configuration initiale

Module 1 : Comprendre l'architecture Juniper Networks et SRX (2h)

Objectifs

- Comprendre le positionnement des pare-feux SRX.
- Identifier les composants de l'architecture Juniper.

Contenu

- Présentation de Juniper Networks.
- Gamme SRX.
- Architecture Junos OS.
- Fonctionnement des pare-feux nouvelle génération.
- Contrôle des flux et segmentation.
- Cas d'usage en entreprise.

Mises en pratique

- Découverte de l'interface Junos.
- Analyse d'une architecture de sécurité.
- Étude de cas d'intégration dans un SI.

Module 2 : Installation et configuration initiale d'un pare-feu SRX (2h)

Objectifs

- Déployer un équipement SRX opérationnel.

Contenu

- Architecture matérielle et virtuelle.
- Configuration initiale.
- Interfaces réseau.
- Configuration des accès administrateurs.
- Sauvegarde de configuration.
- Gestion des mises à jour.

Mises en pratique

- Configuration initiale d'un SRX.
- Paramétrage des interfaces.
- Validation de la connectivité.

Module 3 : Configurer les zones de sécurité et les politiques de filtrage (3h)

Objectifs

- Contrôler les communications réseau.

Contenu

- Security Zones.
- Politiques de sécurité.
- Contrôle des flux.
- Ordonnancement des règles.
- Gestion des applications.
- Bonnes pratiques de filtrage.

Mises en pratique

- Création de zones de sécurité.
- Mise en œuvre de règles de filtrage.
- Validation des flux autorisés et bloqués.

Jour 2 – Routage, NAT et VPN

Module 4 : Configurer le routage et la traduction d'adresses (2h)

Objectifs

- Assurer les communications entre réseaux.

Contenu

- Routage statique.
- Routage dynamique (présentation).
- NAT source.
- NAT destination.
- PAT.
- Publication de services.

Mises en pratique

- Mise en œuvre du routage.
- Configuration NAT.
- Publication sécurisée d'applications.

Module 5 : Mettre en œuvre les VPN IPsec (3h)

Objectifs

- Sécuriser les communications inter-sites.

Contenu

- Concepts IPsec.
- IKE Phase 1 et Phase 2.
- VPN Site-to-Site.
- Authentification.
- Chiffrement.
- Bonnes pratiques de déploiement.

Mises en pratique

- Configuration d'un VPN IPsec.
- Validation de la communication sécurisée.
- Diagnostic des problèmes de connexion.

Module 6 : Configurer les services de sécurité avancés (2h)

Objectifs

- Renforcer la protection du système d'information.

Contenu

- UTM (Unified Threat Management).

- Antivirus.
- Web Filtering.
- IPS.
- Application Security.
- Contrôle des contenus.

Mises en pratique

- Configuration de profils de sécurité.
- Association aux politiques réseau.
- Analyse des événements générés.

Jour 3 – Supervision, diagnostic et exploitation

Module 7 : Superviser les événements et les flux réseau (2h)

Objectifs

- Contrôler l'activité du pare-feu.

Contenu

- Journaux de trafic.
- Journaux de sécurité.
- Monitoring des sessions.
- Rapports.
- Analyse des événements.

Mises en pratique

- Analyse des journaux.
- Recherche d'incidents.
- Construction de rapports d'exploitation.

Module 8 : Diagnostiquer et résoudre les incidents (2h)

Objectifs

- Mettre en œuvre une méthodologie efficace de dépannage.

Contenu

- Outils de diagnostic Junos.
- Analyse des sessions.
- Capture de paquets.
- Diagnostic VPN.
- Diagnostic NAT et routage.

Mises en pratique

- Résolution de problèmes réseau simulés.
- Analyse de flux bloqués.
- Dépannage guidé.

Module 9 : Haute disponibilité et exploitation des pare-feux SRX (2h)

Objectifs

- Garantir la continuité de service.

Contenu

- Concepts de haute disponibilité.
- Chassis Cluster.
- Redondance.
- Sauvegarde et restauration.
- Gestion des mises à jour.
- Maintenance préventive.

Mises en pratique

- Présentation d'un cluster SRX.
- Sauvegarde de configuration.
- Planification d'une maintenance.

Module 10 : Atelier fil rouge – Déploiement d'une architecture sécurisée Juniper SRX (1h)

Objectifs

- Mettre en œuvre l'ensemble des compétences acquises.

Contenu

- Déploiement d'une architecture comprenant :
  - zones de sécurité
  - routage
  - NAT
  - VPN IPsec
  - politiques de sécurité
  - supervision

Mises en pratique

- Étude de cas complète d'entreprise.
- Déploiement et validation de la configuration.
- Analyse des événements de sécurité.
- Résolution d'incidents simulés.
- Évaluation pratique finale.
- Débriefing collectif et synthèse des acquis.

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à mailto:referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.