PARE-FEUX PALO ALTO

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 et de pare-feu recommandées.
- Expérience en administration systèmes ou réseaux appréciée.

PROFIL DES STAGIAIRES

- Administrateurs réseaux.
- Administrateurs sécurité.
- Ingénieurs systèmes et réseaux.
- Ingénieurs cybersécurité.
- Responsables infrastructures souhaitant administrer des pare-feux Palo Alto Networks.

OBJECTIFS

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

- Comprendre l'architecture des pare-feux Palo Alto Networks.
- Configurer les interfaces et zones de sécurité.
- Mettre en œuvre les politiques de sécurité.
- Configurer la traduction d'adresses (NAT).
- Administrer les profils de sécurité avancés.
- Analyser les journaux et événements de sécurité.
- Diagnostiquer les incidents réseau et sécurité.
- Assurer l'exploitation quotidienne d'un pare-feu Palo Alto.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Présentations théoriques.
- Démonstrations techniques.
- Travaux pratiques sur environnement Palo Alto.
- Études de cas de sécurité réseau.
- Exercices de configuration.
- Ateliers de dépannage et d'analyse de trafic.

FORMATEUR

- Consultant formateur expert en cybersécurité et infrastructures réseau disposant d'une expérience significative dans le déploiement et l'administration de solutions Palo Alto 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 et configuration de l'infrastructure Palo Alto

Module 1 : Comprendre l'architecture Palo Alto Networks (2h)

Objectifs

- Comprendre le fonctionnement des pare-feux nouvelle génération (NGFW).
- Identifier les composants d'une architecture Palo Alto.

Contenu

- Présentation de Palo Alto Networks.
- Architecture NGFW.
- Fonctionnement App-ID.
- Fonctionnement User-ID.
- Fonctionnement Content-ID.
- Positionnement dans une architecture de sécurité.
- Cas d'usage d'entreprise.

Mises en pratique

- Découverte de l'interface d'administration.
- Analyse d'une architecture de sécurité.
- Brainstorming sur les besoins de filtrage et de contrôle.

Module 2 : Configuration initiale du pare-feu (2h)

Objectifs

- Réaliser la mise en service d'un pare-feu Palo Alto.

Contenu

- Configuration des interfaces.
- Gestion des zones de sécurité.
- Configuration des routes.
- Administration des accès.
- Sauvegarde de configuration.
- Gestion des licences et mises à jour.

Mises en pratique

- Configuration initiale d'un pare-feu.
- Création des zones réseau.
- Vérification de la connectivité.

Module 3 : Mettre en œuvre les politiques de sécurité (3h)

Objectifs

- Contrôler les flux réseau selon les règles de sécurité.

Contenu

- Principes des Security Policies.
- Gestion des règles de sécurité.
- Contrôle applicatif.
- Contrôle des utilisateurs.
- Ordonnancement des règles.
- Bonnes pratiques de filtrage.

Mises en pratique

- Création de politiques de sécurité.
- Autorisation et blocage d'applications.
- Validation des flux autorisés.

Jour 2 – Contrôle avancé et protection des flux

Module 4 : Configurer la traduction d'adresses (NAT) (2h)

Objectifs

- Gérer les mécanismes de publication et de traduction d'adresses.

Contenu

- NAT source.
- NAT destination.
- PAT.
- Publication de services.
- Bonnes pratiques.

Mises en pratique

- Configuration de règles NAT.
- Publication d'un serveur interne.
- Validation des traductions.

Module 5 : Exploiter les technologies App-ID et User-ID (2h)

Objectifs

- Contrôler précisément les usages réseau.

Contenu

- Identification applicative.
- Classification des applications.
- Intégration Active Directory.
- User-ID.
- Contrôle basé sur les utilisateurs.

Mises en pratique

- Création de politiques basées sur les applications.
- Mise en œuvre du contrôle utilisateur.
- Analyse des comportements applicatifs.

Module 6 : Configurer les profils de sécurité avancés (3h)

Objectifs

- Renforcer la protection des utilisateurs et des systèmes.

Contenu

- Antivirus.
- Anti-spyware.
- Vulnérability Protection.
- URL Filtering.

- File Blocking.
- WildFire (présentation).
- Security Profiles.

Mises en pratique

- Création de profils de sécurité.
- Association aux politiques réseau.
- Simulation de détection de menaces.

Jour 3 – Supervision, diagnostic et exploitation

Module 7 : Analyser les journaux et les événements de sécurité (2h)

Objectifs

- Exploiter les capacités de supervision du pare-feu.

Contenu

- Traffic Logs.
- Threat Logs.
- URL Logs.
- ACC (Application Command Center).
- Tableaux de bord.
- Reporting.

Mises en pratique

- Analyse de journaux de sécurité.
- Recherche d'événements.
- Construction de rapports.

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

Objectifs

- Mettre en œuvre une méthodologie efficace de dépannage.

Contenu

- Diagnostic réseau.
- Analyse des sessions.
- Packet Capture.
- Outils de troubleshooting.
- Résolution des incidents courants.

Mises en pratique

- Résolution d'incidents simulés.
- Analyse de flux bloqués.
- Utilisation des outils de diagnostic.

Module 9 : Administration avancée et bonnes pratiques d'exploitation (2h)

Objectifs

- Assurer le maintien en conditions opérationnelles.

Contenu

- Gestion des administrateurs.
- Sauvegardes.
- Mise à jour PAN-OS.
- Haute disponibilité (présentation).
- Gestion des changements.
- Documentation d'exploitation.

Mises en pratique

- Gestion des profils administrateurs.

- Sauvegarde et restauration.
- Préparation d'un plan de maintenance.

Module 10 : Atelier fil rouge – Déploiement d'une politique de sécurité complète (1h)

Objectifs

- Mettre en œuvre l'ensemble des compétences acquises.

Contenu

- Création d'une architecture de sécurité comprenant :
  - zones réseau
  - routage
  - NAT
  - politiques de sécurité
  - profils de protection
  - supervision

Mises en pratique

- Étude de cas complète d'entreprise.
- Déploiement et validation des politiques.
- Analyse des événements générés.
- 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.