PARE-FEUX FORTINET NSE4

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.
- Expérience en administration systèmes ou réseaux appréciée.

PROFIL DES STAGIAIRES

- Administrateurs réseaux.
- Administrateurs sécurité.
- Ingénieurs systèmes et réseaux.
- Ingénieurs cybersécurité.
- Exploitants d'infrastructures.
- Toute personne souhaitant administrer des équipements FortiGate et préparer le niveau NSE4.

OBJECTIFS

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

- Comprendre l'architecture de sécurité Fortinet.
- Installer et configurer un pare-feu FortiGate.
- Administrer les interfaces, zones et politiques de sécurité.
- Mettre en œuvre le NAT et le routage.
- Configurer les services VPN.
- Déployer les mécanismes de protection avancés.
- Superviser et analyser les événements de sécurité.
- Diagnostiquer les incidents réseau et sécurité.
- Se préparer aux concepts abordés dans la certification Fortinet NSE4.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Présentations théoriques.
- Démonstrations techniques.
- Travaux pratiques sur équipements FortiGate.
- Études de cas.
- Exercices de configuration.
- Ateliers de diagnostic et de dépannage.

FORMATEUR

- Consultant formateur expert Fortinet et cybersécurité disposant d'une expérience significative dans le déploiement et l'administration de solutions FortiGate 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 – Architecture Fortinet et configuration initiale

Module 1 : Comprendre l'architecture de sécurité Fortinet (2h)

Objectifs

- Comprendre l'écosystème Fortinet.
- Identifier les composants d'une architecture FortiGate.

Contenu

- Présentation de Fortinet Security Fabric.
- Positionnement de FortiGate dans le SI.
- Fonctionnement d'un pare-feu nouvelle génération.
- Contrôle applicatif.
- Inspection du trafic.
- Intégration dans une architecture de sécurité.

Mises en pratique

- Découverte de l'interface FortiOS.
- Analyse d'une architecture de sécurité d'entreprise.
- Étude de cas de segmentation réseau.

Module 2 : Installation et configuration initiale de FortiGate (2h)

Objectifs

- Mettre en service un pare-feu FortiGate.

Contenu

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

Mises en pratique

- Configuration initiale d'un FortiGate.
- Paramétrage des interfaces.
- Vérification de la connectivité.

Module 3 : Routage, politiques de sécurité et NAT (3h)

Objectifs

- Contrôler les flux réseau et les accès.

Contenu

- Routage statique.
- Politiques de sécurité.
- Ordonnancement des règles.
- NAT source.
- NAT destination.
- Publication de services.

Mises en pratique

- Création de politiques de filtrage.
- Mise en œuvre du NAT.
- Publication sécurisée d'un serveur interne.
- Validation des flux autorisés.

Jour 2 – Services avancés et sécurité renforcée

Module 4 : Authentification et gestion des accès utilisateurs (2h)

Objectifs

- Contrôler l'accès aux ressources réseau.

Contenu

- Comptes administrateurs.
- Authentification locale.
- Intégration Active Directory.
- LDAP.
- RADIUS.
- Contrôle basé sur les utilisateurs.

Mises en pratique

- Intégration à un annuaire.
- Création de profils d'administration.
- Mise en œuvre du contrôle utilisateur.

Module 5 : Configurer les VPN IPsec et SSL VPN (3h)

Objectifs

- Sécuriser les communications distantes.

Contenu

- Principes des VPN.
- VPN IPsec Site-to-Site.
- VPN IPsec Remote Access.
- SSL VPN.
- Authentification des utilisateurs.
- Bonnes pratiques de sécurisation.

Mises en pratique

- Mise en œuvre d'un VPN IPsec.
- Configuration d'un accès SSL VPN.
- Validation de la connectivité sécurisée.

Module 6 : Mettre en œuvre les services de sécurité avancés (2h)

Objectifs

- Renforcer la protection des utilisateurs et des systèmes.

Contenu

- Antivirus.

- IPS (Intrusion Prevention System).
- Web Filtering.
- Application Control.
- DNS Filtering.
- Protection contre les menaces avancées.

Mises en pratique

- Configuration des profils de sécurité.
- Association aux politiques de sécurité.
- Analyse des détections générées.

Jour 3 – Supervision, diagnostic et exploitation

Module 7 : Superviser les événements et analyser le trafic (2h)

Objectifs

- Exploiter les outils de supervision Fortinet.

Contenu

- Journaux et événements.
- Tableaux de bord.
- Monitoring temps réel.
- Rapports de sécurité.
- Analyse des sessions.

Mises en pratique

- Analyse des journaux de trafic.
- Recherche d'événements de sécurité.
- Création de rapports d'exploitation.

Module 8 : Diagnostiquer les incidents réseau et sécurité (2h)

Objectifs

- Résoudre efficacement les incidents.

Contenu

- Outils de diagnostic FortiOS.
- Analyse des sessions.
- Capture de paquets.
- Diagnostic VPN.
- Résolution des problèmes de routage et de sécurité.

Mises en pratique

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

Module 9 : Haute disponibilité et bonnes pratiques d'exploitation (2h)

Objectifs

- Assurer la disponibilité des services de sécurité.

Contenu

- Concepts de haute disponibilité (HA).
- Clusters FortiGate.
- Sauvegarde et restauration.
- Gestion des mises à jour FortiOS.
- Maintenance préventive.
- Bonnes pratiques d'exploitation.

Mises en pratique

- Configuration d'un cluster HA.
- Sauvegarde et restauration de configuration.
- Planification des opérations de maintenance.

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

Objectifs

- Mettre en œuvre l'ensemble des compétences acquises.

Contenu

- Déploiement d'une infrastructure comprenant :
  - Interfaces et routage
  - NAT
  - Politiques de sécurité
  - VPN
  - Profils de sécurité
  - Supervision

Mises en pratique

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