EduGroupe
Accompagner pour réussir

PROXY McAfee

Durée : 3 jours (21 heures)

CONNAISSANCES PREALABLES

- Connaissances fondamentales des réseaux TCP/IP.
- Compréhension des protocoles HTTP, HTTPS, DNS et SSL/TLS.
- Notions de sécurité réseau et de filtrage Web.
- Expérience en administration systèmes ou réseaux recommandée.

PROFIL DES STAGIAIRES

- Administrateurs sécurité.
- Administrateurs réseaux.
- Administrateurs systèmes.
- Ingénieurs cybersécurité.
- Exploitants d'infrastructures de sécurité.
- Responsables de la sécurité des accès Internet.

OBJECTIFS

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

- Comprendre l'architecture McAfee Web Gateway.
- Installer et configurer une plateforme de proxy Web sécurisé.
- Mettre en œuvre des politiques de filtrage Internet.
- Configurer l'authentification des utilisateurs.
- Déployer l'inspection SSL/TLS.
- Contrôler les usages Web et les applications Internet.
- Superviser les accès et les événements de sécurité.
- Diagnostiquer les incidents liés au filtrage Web.
- Assurer l'exploitation quotidienne d'une infrastructure McAfee Web Gateway.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Présentations théoriques.
- Démonstrations techniques.
- Travaux pratiques sur plateforme McAfee Web Gateway.
- Études de cas.
- Exercices de configuration.
- Ateliers de diagnostic et de dépannage.

FORMATEUR

- Consultant formateur expert cybersécurité et sécurité Web disposant d'une expérience significative dans le déploiement et l'administration de solutions McAfee Web Gateway 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 McAfee Web Gateway

Module 1 : Comprendre l'architecture McAfee Web Gateway (2h)

Objectifs

- Comprendre le rôle d'un Secure Web Gateway.
- Identifier les composants d'une architecture McAfee Web Gateway.

Contenu

- Présentation de McAfee Web Gateway.
- Fonctionnement d'un proxy Web sécurisé.
- Architecture Secure Web Gateway.
- Proxy explicite et proxy transparent.
- Contrôle des flux Internet.
- Positionnement dans une architecture de cybersécurité.

Mises en pratique

- Découverte de l'interface d'administration.
- Analyse d'une architecture de sécurité Web.
- Étude de cas d'intégration dans une entreprise.

Module 2 : Installer et configurer la plateforme (2h)

Objectifs

- Déployer une solution McAfee Web Gateway opérationnelle.

Contenu

- Architecture de déploiement.
- Configuration réseau.
- Interfaces et passerelles.
- Paramétrage système.
- Gestion des administrateurs.
- Sauvegarde et restauration.

Mises en pratique

- Configuration initiale de la plateforme.
- Paramétrage réseau.
- Validation de la connectivité.

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

Objectifs

- Contrôler les accès Internet des utilisateurs.

Contenu

- Policy Engine.
- Catégorisation Web.
- Création de règles de filtrage.
- Gestion des exceptions.
- Blocage des contenus.
- Bonnes pratiques de sécurisation.

Mises en pratique

- Création de politiques de filtrage.
- Autorisation et blocage de catégories Web.
- Validation des règles de sécurité.

Jour 2 – Authentification, SSL et contrôle avancé

Module 4 : Intégrer les utilisateurs et les annuaires d'entreprise (2h)

Objectifs

- Appliquer les politiques selon l'identité des utilisateurs.

Contenu

- Authentification utilisateur.
- Active Directory.
- LDAP.
- Groupes de sécurité.
- Single Sign-On.
- Contrôle basé sur les utilisateurs.

Mises en pratique

- Connexion à Active Directory.
- Création de règles basées sur les groupes.
- Validation de l'authentification.

Module 5 : Configurer l'inspection SSL/TLS (3h)

Objectifs

- Contrôler les flux HTTPS.

Contenu

- Fonctionnement SSL/TLS.
- SSL Scanner.
- Gestion des certificats.
- Déchiffrement du trafic HTTPS.
- Gestion des exceptions.
- Contraintes réglementaires et techniques.

Mises en pratique

- Déploiement des certificats.
- Configuration de l'inspection SSL.
- Analyse du trafic HTTPS.

Module 6 : Contrôle applicatif et sécurisation des usages Internet (2h)

Objectifs

- Contrôler les applications et les usages Web.

Contenu

- Contrôle applicatif.

- Réseaux sociaux.
- Applications SaaS.
- Streaming.
- Téléchargements.
- Gestion des risques utilisateurs.

Mises en pratique

- Création de politiques applicatives.
- Contrôle des usages Internet.
- Analyse des comportements utilisateurs.

Jour 3 – Supervision, diagnostic et exploitation

Module 7 : Superviser les accès Web et analyser les événements (2h)

Objectifs

- Exploiter les informations de supervision.

Contenu

- Journaux de navigation.
- Tableaux de bord.
- Rapports d'activité.
- Alertes de sécurité.
- Analyse des tendances.

Mises en pratique

- Analyse des journaux Web.
- Création de rapports.
- Identification des usages à risque.

Module 8 : Diagnostiquer les incidents liés au proxy Web (2h)

Objectifs

- Résoudre efficacement les problèmes de navigation.

Contenu

- Analyse des flux HTTP/HTTPS.
- Diagnostic SSL.
- Analyse des refus d'accès.
- Résolution des problèmes d'authentification.
- Méthodologie de dépannage.

Mises en pratique

- Résolution d'incidents simulés.
- Dépannage de problèmes de navigation.
- Analyse de flux bloqués.

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

Objectifs

- Assurer le maintien en conditions opérationnelles.

Contenu

- Gestion des administrateurs.
- Sauvegarde et restauration.
- Mises à jour.
- Gestion des changements.
- Documentation d'exploitation.
- Durcissement de la plateforme.

Mises en pratique

- Gestion des profils administrateurs.
- Sauvegarde complète de la configuration.
- Préparation d'un plan de maintenance.

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

Objectifs

- Mettre en œuvre l'ensemble des compétences acquises.

Contenu

- Déploiement d'une architecture comprenant :
  - authentification Active Directory
  - filtrage Web
  - inspection SSL
  - contrôle applicatif
  - supervision
  - reporting

Mises en pratique

- Étude de cas complète d'entreprise.
- Déploiement des politiques de sécurité.
- 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.