PROXY SKYHIGH

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.
- Ingénieurs cybersécurité.
- Administrateurs systèmes.
- Exploitants de solutions de sécurité Web.
- Responsables de la sécurité des accès Internet.

OBJECTIFS

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

- Comprendre l'architecture des solutions Skyhigh Secure Web Gateway.
- Installer et configurer un proxy Web Skyhigh.
- Mettre en œuvre les politiques de filtrage Web.
- Contrôler les accès Internet des utilisateurs.
- Configurer l'authentification et l'intégration Active Directory.
- Déployer l'inspection SSL/TLS.
- Superviser et analyser les activités Web.
- Diagnostiquer les incidents liés au filtrage et à la navigation Internet.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Présentations théoriques.
- Démonstrations techniques.
- Travaux pratiques sur environnement Skyhigh Secure Web Gateway.
- Études de cas.
- Exercices de configuration.
- Ateliers de diagnostic et d'analyse de trafic.

FORMATEUR

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

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 Skyhigh Secure Web Gateway et configuration initiale

Module 1 : Comprendre l'architecture Skyhigh Security (2h)

Objectifs

- Comprendre le rôle d'un Secure Web Gateway.
- Identifier les composants de l'architecture Skyhigh.

Contenu

- Présentation de Skyhigh Security.
- Évolution de McAfee Web Gateway vers Skyhigh.
- Architecture Secure Web Gateway (SWG).
- Proxy explicite et proxy transparent.
- Protection des accès Internet.
- Cas d'usage d'entreprise.

Mises en pratique

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

Module 2 : Installer et configurer le proxy Skyhigh (2h)

Objectifs

- Déployer une plateforme Skyhigh opérationnelle.

Contenu

- Architecture de déploiement.
- Configuration réseau.
- Paramètres système.
- Gestion des interfaces.
- Paramétrage des accès administrateurs.
- Sauvegarde et restauration.

Mises en pratique

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

Module 3 : Mettre en œuvre le filtrage Web (3h)

Objectifs

- Contrôler les accès Internet des utilisateurs.

Contenu

- Catégorisation des sites Web.
- Règles de filtrage.
- Gestion des politiques d'accès.
- Contrôle des applications Web.
- Gestion des exceptions.
- Bonnes pratiques de filtrage.

Mises en pratique

- Création de politiques de filtrage.
- Blocage et autorisation de catégories.
- Validation des règles de sécurité.

Jour 2 – Authentification, SSL et contrôle avancé

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

Objectifs

- Associer les règles de sécurité aux utilisateurs.

Contenu

- Authentification des utilisateurs.
- Active Directory.
- LDAP.
- Single Sign-On.
- Gestion des groupes.
- Politiques basées sur les identités.

Mises en pratique

- Connexion à un annuaire Active Directory.
- Création de politiques par groupes utilisateurs.
- Validation de l'authentification.

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

Objectifs

- Contrôler les flux HTTPS.

Contenu

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

Mises en pratique

- Déploiement de certificats.
- Activation de l'inspection SSL.
- Analyse des flux HTTPS.

Module 6 : Contrôler les applications et les usages Web (2h)

Objectifs

- Renforcer le contrôle des usages Internet.

Contenu

- Contrôle applicatif.
- Applications SaaS.
- Réseaux sociaux.

- Streaming.
- Téléchargements.
- Gestion des risques utilisateurs.

Mises en pratique

- Création de politiques applicatives.
- Limitation d'usages spécifiques.
- Analyse des comportements utilisateurs.

Jour 3 – Supervision, diagnostic et exploitation

Module 7 : Superviser les accès Internet et générer des rapports (2h)

Objectifs

- Exploiter les informations de supervision.

Contenu

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

Mises en pratique

- Analyse des journaux de navigation.
- 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

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

Mises en pratique

- Analyse d'incidents simulés.
- Résolution de problèmes de navigation.
- Dépannage SSL et authentification.

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

Objectifs

- Assurer le maintien en conditions opérationnelles.

Contenu

- Gestion des administrateurs.
- Sauvegardes.
- Mises à jour.
- Gestion des changements.
- Documentation d'exploitation.
- Bonnes pratiques de sécurité.

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 Web complète (1h)

Objectifs

- Mettre en œuvre l'ensemble des compétences acquises.

Contenu

- Déploiement d'une architecture comprenant :
  - authentification AD
  - 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.