EduGroupe
Accompagner pour réussir

PROXY BLUECOAT

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 réseaux.
- Administrateurs sécurité.
- 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 des solutions ProxySG (Blue Coat / Symantec).
- Installer et configurer un proxy Web ProxySG.
- 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.
- Superviser les accès Internet et les événements de sécurité.
- Diagnostiquer les incidents liés au proxy et à la navigation Web.
- Assurer l'exploitation quotidienne d'une infrastructure ProxySG.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Présentations théoriques.
- Démonstrations techniques.
- Travaux pratiques sur plateforme ProxySG.
- Études de cas.
- Exercices de configuration.
- Ateliers d'analyse et de dépannage.

FORMATEUR

- Consultant formateur expert cybersécurité et sécurité Web disposant d'une expérience significative dans le déploiement et l'administration de solutions ProxySG / Blue Coat en environnement de production.

METHODE D'EVALUATION DES ACQUIS

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

CONTENU DU COURS

Jour 1 – Découverte de ProxySG et mise en œuvre initiale

Module 1 : Comprendre l'architecture ProxySG (2h)

Objectifs

- Comprendre le rôle d'un proxy Web sécurisé.
- Identifier les composants d'une architecture ProxySG.

Contenu

- Présentation de Blue Coat et Symantec ProxySG.
- Rôle d'un Secure Web Gateway.
- Architecture ProxySG.
- Proxy explicite et transparent.
- Flux Web entrants et sortants.
- Positionnement dans une architecture de sécurité.

Mises en pratique

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

Module 2 : Installation et configuration initiale du ProxySG (2h)

Objectifs

- Déployer un environnement ProxySG opérationnel.

Contenu

- Configuration réseau.
- Interfaces et connectivité.
- Paramètres système.
- Gestion des accès administrateurs.
- Sauvegarde et restauration.
- Gestion des licences.

Mises en pratique

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

Module 3 : Configurer les politiques de filtrage Web (3h)

Objectifs

- Contrôler les accès Internet.

Contenu

- Concepts de Policy Engine.
- Catégorisation Web.
- Règles de filtrage.
- Gestion des exceptions.
- Contrôle des téléchargements.
- Bonnes pratiques de filtrage.

Mises en pratique

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

Jour 2 – Contrôle des utilisateurs et inspection SSL

Module 4 : Authentification et intégration aux annuaires (2h)

Objectifs

- Appliquer les politiques selon les profils utilisateurs.

Contenu

- Authentification utilisateur.
- Active Directory.
- LDAP.
- Single Sign-On.
- Groupes de sécurité.
- Politiques basées sur l'identité.

Mises en pratique

- Intégration à Active Directory.
- Création de règles par groupes utilisateurs.
- Validation des authentifications.

Module 5 : Mettre en œuvre l'inspection SSL/TLS (3h)

Objectifs

- Contrôler les flux HTTPS.

Contenu

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

Mises en pratique

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

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

Objectifs

- Contrôler les usages Internet avancés.

Contenu

- Contrôle applicatif.

- Applications SaaS.
- Réseaux sociaux.
- Streaming et multimédia.
- Gestion des risques utilisateurs.
- Limitation des usages non conformes.

Mises en pratique

- Création de règles applicatives.
- Contrôle des applications Web.
- Analyse des comportements utilisateurs.

Jour 3 – Supervision, diagnostic et exploitation

Module 7 : Superviser les accès Internet et les événements de sécurité (2h)

Objectifs

- Exploiter les outils de supervision ProxySG.

Contenu

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

Mises en pratique

- Analyse des journaux de navigation.
- Création de rapports.
- Identification des comportements à risque.

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

Objectifs

- Résoudre efficacement les problèmes de navigation.

Contenu

- Diagnostic des flux HTTP/HTTPS.
- Analyse des refus d'accès.
- Diagnostic de l'authentification.
- Dépannage SSL.
- Méthodologie de résolution d'incidents.

Mises en pratique

- Analyse d'incidents simulés.
- Dépannage des problèmes d'accès Web.
- Résolution d'incidents d'authentification.

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

Objectifs

- Maintenir un environnement ProxySG en conditions opérationnelles.

Contenu

- Gestion des administrateurs.
- Sauvegardes.
- Mises à jour logicielles.
- Gestion des changements.
- Documentation d'exploitation.
- Durcissement de la plateforme.

Mises en pratique

- Gestion des profils administrateurs.
- Sauvegarde et restauration.
- Élaboration 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
  - reporting
  - supervision

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.