EduGroupe
Accompagner pour réussir

PROXY ZSCALER

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.
- Connaissances générales des architectures Cloud recommandées.

PROFIL DES STAGIAIRES

- Administrateurs sécurité.
- Administrateurs réseaux.
- Ingénieurs cybersécurité.
- Administrateurs systèmes.
- Architectes sécurité.
- Responsables de la sécurité des accès Internet et du modèle Zero Trust.

OBJECTIFS

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

- Comprendre l'architecture Zscaler Internet Access (ZIA).
- Déployer et administrer une solution de proxy Cloud Zscaler.
- Mettre en œuvre des politiques de filtrage Web et applicatif.
- Configurer l'authentification et l'intégration avec les annuaires d'entreprise.
- Déployer l'inspection SSL/TLS.
- Contrôler les usages Internet et SaaS.
- Superviser les activités utilisateurs et les événements de sécurité.
- Diagnostiquer les incidents liés à la navigation et aux politiques de sécurité.
- Comprendre les principes du Secure Service Edge (SSE) et du Zero Trust.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

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

FORMATEUR

- Consultant formateur expert cybersécurité, SSE et architectures Cloud Security disposant d'une expérience significative dans le déploiement et l'administration de solutions Zscaler en environnement d'entreprise.

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 Zscaler et mise en œuvre de l'architecture

Module 1 : Comprendre l'architecture Zscaler Internet Access (2h)

Objectifs

- Comprendre les concepts de Secure Service Edge (SSE).
- Identifier les composants de l'architecture Zscaler.

Contenu

- Présentation de Zscaler.
- Concepts Zero Trust.
- Secure Service Edge (SSE).
- Secure Access Service Edge (SASE).
- Architecture Cloud Native.
- Fonctionnement de ZIA.
- Cas d'usage d'entreprise.

Mises en pratique

- Découverte de la console d'administration.
- Analyse d'une architecture Zscaler.
- Étude de cas de migration d'un proxy traditionnel vers le Cloud.

Module 2 : Déployer et configurer ZIA (2h)

Objectifs

- Mettre en service une plateforme Zscaler.

Contenu

- Architecture de déploiement.
- Gestion des emplacements (Locations).
- Tunnel GRE.
- Tunnel IPsec.
- Zscaler Client Connector.
- Paramétrage des accès administrateurs.

Mises en pratique

- Création d'un emplacement d'entreprise.
- Configuration d'un tunnel sécurisé.
- Validation du trafic vers Zscaler.

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

Objectifs

- Contrôler les accès Internet des utilisateurs.

Contenu

- URL Filtering.
- Catégorisation Web.
- Politiques d'accès.
- Gestion des exceptions.
- Contrôle des téléchargements.
- Contrôle des contenus.

Mises en pratique

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

Jour 2 – Contrôle des utilisateurs, SSL et applications Cloud

Module 4 : Authentification et intégration avec les annuaires (2h)

Objectifs

- Appliquer les politiques selon l'identité des utilisateurs.

Contenu

- Intégration Active Directory.
- Azure AD.
- LDAP.
- SAML.
- Single Sign-On.
- Groupes et profils utilisateurs.

Mises en pratique

- Connexion à un fournisseur d'identité.
- Configuration du SSO.
- Validation de l'authentification des utilisateurs.

Module 5 : Inspection SSL/TLS et protection avancée (3h)

Objectifs

- Contrôler et sécuriser les flux chiffrés.

Contenu

- Architecture SSL Inspection.
- Gestion des certificats.
- Déchiffrement HTTPS.
- Exceptions SSL.
- Protection contre les menaces.
- Contraintes réglementaires.

Mises en pratique

- Déploiement du certificat racine.
- Activation de l'inspection SSL.
- Analyse des flux HTTPS.

Module 6 : Contrôle des applications SaaS et Cloud (2h)

Objectifs

- Maîtriser les usages Cloud des utilisateurs.

Contenu

- Cloud Application Control.
- Shadow IT.
- Contrôle des applications SaaS.
- Microsoft 365.
- Google Workspace.
- Gestion des risques applicatifs.

Mises en pratique

- Création de politiques applicatives.
- Contrôle des usages SaaS.
- Analyse des applications découvertes.

Jour 3 – Supervision, diagnostic et exploitation

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

Objectifs

- Exploiter les capacités d'analyse de Zscaler.

Contenu

- Journaux de navigation.
- Dashboards.
- Rapports d'activité.
- Alertes.
- Analyse des comportements utilisateurs.

Mises en pratique

- Analyse des journaux d'activité.
- Création de rapports personnalisés.
- Identification des usages à risque.

Module 8 : Diagnostiquer les incidents et optimiser l'expérience utilisateur (2h)

Objectifs

- Résoudre efficacement les problèmes de navigation.

Contenu

- Diagnostic des flux Internet.
- Analyse des refus d'accès.
- Dépannage SSL.
- Résolution des problèmes d'authentification.
- Optimisation des performances.

Mises en pratique

- Résolution d'incidents simulés.
- Analyse de flux bloqués.
- Dépannage des politiques de sécurité.

Module 9 : Administration avancée et bonnes pratiques Zero Trust (2h)

Objectifs

- Maintenir une plateforme Zscaler performante et sécurisée.

Contenu

- Gestion des administrateurs.
- RBAC (Role Based Access Control).
- Gestion des changements.
- Audit de configuration.
- Bonnes pratiques d'exploitation.
- Gouvernance des politiques Zero Trust.

Mises en pratique

- Création de rôles administratifs.
- Revue de configuration.
- Élaboration d'un plan de gouvernance.

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

Objectifs

- Mettre en œuvre l'ensemble des compétences acquises.

Contenu

- Déploiement d'une architecture comprenant :
  - authentification SSO
  - filtrage Web
  - inspection SSL
  - contrôle SaaS
  - supervision
  - reporting
  - gouvernance Zero Trust

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.