Fortinet

FORTINET

Découvrez notre formation spécialisée sur Fortinet, conçue pour vous offrir une expertise approfondie dans la gestion des solutions de sécurité réseau. Apprenez à déployer, configurer et optimiser les appareils FortiGate pour renforcer la protection de votre infrastructure contre les menaces numériques.

Présentiel - Synchrone

Objectifs

1. Maîtriser la configuration et l'administration des pare-feu FortiGate, en comprenant en détail leur architecture et leurs fonctionnalités.
2. Mettre en œuvre des stratégies de filtrage réseau et applicatif avancées pour renforcer la sécurité des infrastructures informatiques.
3. Configurer et gérer des VPN sécurisés (IPSEC et SSL) ainsi que des fonctionnalités de haute disponibilité pour assurer la continuité des opérations réseau.
4.
5.
6.

Public Visé

Ingénieurs Réseau, Administrateurs Systèmes, Professionnels de la Sécurité de l'Information , Consultants en Sécurité Informatique

Pré Requis

Connaissances de base en réseau : Comprendre les concepts de base des réseaux informatiques, tels que les protocoles TCP/IP, les commutateurs, les routeurs et les pare-feu.

Compétences en systèmes d'exploitation : Avoir une bonne compréhension des systèmes d'exploitation courants, en particulier Linux et Windows.

Les + métier

Cette formation complète sur Fortinet vous offre une immersion pratique dans la configuration et l'administration des pare-feu FortiGate. Explorez les principes fondamentaux des technologies de sécurité réseau, apprenez à mettre en œuvre des stratégies de filtrage avancées, à configurer des VPN sécurisés et à garantir la haute disponibilité de vos infrastructures.

Objectifs pédagogiques et d'évaluation

Expliquer les capacités offertes par le FortiGate
Effectuer l'installation et la configuration du pare-feu (firewall)
Déployer une stratégie de filtrage réseau et d'application
Configurer et gérer les VPN SSL et IPSEC
Mettre en place la haute disponibilité des appareils FortiGate

Méthodes pédagogiques

Démos et Labs
Exercices Pratiques
Sessions de Questions-Réponses

Parcours pédagogique

1. Introduction :
   - Exploration des technologies et des caractéristiques des pare-feu.
   - Présentation de l'architecture et de la gamme des produits Fortinet.
   - Analyse des composants de l'Appliance.
1. Configuration et administration :
   - Apprentissage des tâches administratives et des modes d'administration CLI/GUI et FortiManager.
   - Installation pratique et familiarisation avec l'interface utilisateur.
1. Filtrage réseau et applicatif :
   - Élaboration de politiques de contrôle d'accès et gestion des règles.
   - Mise en œuvre de stratégies de filtrage de contenu, d'URL et anti-spam.
   - Configuration des profils de protection antivirus.
1. NAT et routage :
   - Utilisation des modes NAT/Route/Transparent.
   - Configuration du routage statique et dynamique.
1. VLAN et Virtual Domains (VDOM) :
   - Installation et configuration de VLAN et VDOM.
   - Gestion du routage InterVDOM.
1. VPN avec IPSEC :
   - Configuration des tunnels IPSEC, notamment les modes site à site et client à site.
   - Utilisation du client FortiClient et authentification Xauth.
1. VPN avec SSL :
   - Configuration des tunnels SSL en mode tunnel et portail.

STRATEGIE INFORMATIQUE - Numéro de déclaration d'activité (ne vaut pas agrément de l'état) : 95970120697

Stratégie Informatique
Guadeloupe : Immeuble la Coupole, Grand-Camp 97142 ABYMES Tél : 05 90 83 06 18 Fax : 05 90 83 46 71
Martinique : Immeuble Sera n°6, Zone de Manhity 97232 LAMENTIN Tél : 05 96 57 40 20 Fax : 05 96 51 60 53
SARL AU CAPITAL DE 7775€ - SIRET 352 717 193 00044-APE 6202 A

1. Haute disponibilité :
   - Compréhension des concepts de haute disponibilité et mise en œuvre du mode actif-passif/actif-actif.

Modalités de suivi

Si la formation se déroule tout ou partie en distanciel :
Formation en distanciel via TEAMS. Le participant reçoit une invitation par mail avec le lien de connexion. Le premier jour de l'action de formation, la conseillère assure la présentation des participants et du formateur, de la formation, des outils d'émargement et d'évaluation puis le formateur prend le relai et démarre la formation. Le dernier jour, la conseillère procède à la clôture de la session avec le formateur et les participants.

Moyens pédagogiques

1 ordinateur par stagiaire
Salle de formation claire, climatisée et spacieuse
Tableau blanc
Vidéo projecteur
Support de cours
Environnement de formation installé sur les postes de travail ou en ligne

Qualification Intervenant·e·s

Formateur - consultant expert sur Fortinet

Méthodes et modalités d'évaluation

Evaluation diagnostique en amont : questionnaire d'auto-positionnement et recueil des attentes & besoins - Evaluation formative en cours de formation : exercices - Evaluation sommative en fin de formation : exercice/QCM - Bilan individuel des compétences acquises - Questionnaire de satisfaction à chaud - Questionnaire de satisfaction à froid

Modalités d'accessibilité handicap

Pour les personnes en situation de handicap, et en fonction des besoins spécifiques, un entretien avec notre référente handicap pourra être organisé. Vous pourrez vous exprimer en toute confidentialité et liberté sur votre handicap. Merci de noter ci-dessous si vous êtes en situation de handicap.

Durée

28.00 Heures **4** Jours

Effectif

De 3 à 8 Personnes

STRATEGIE INFORMATIQUE - Numéro de déclaration d'activité (ne vaut pas agrément de l'état) : 95970120697

Stratégie Informatique
Guadeloupe : Immeuble la Coupole, Grand-Camp 97142 ABYMES Tél : 05 90 83 06 18 Fax : 05 90 83 46 71
Martinique : Immeuble Sera n°6, Zone de Manhity 97232 LAMENTIN Tél : 05 96 57 40 20 Fax : 05 96 51 60 53
SARL AU CAPITAL DE 7775€ - SIRET 352 717 193 00044-APE 6202 A