Plan de cours N° : 651
Durée : 4 jours (28h)

FORTINET
Installation et configuration d'un firewall FortiGate

PARTICIPANTS / PRE-REQUIS

Techniciens, ingénieurs systèmes/réseaux/sécurité et administrateurs.

Bonnes connaissances de TCP/IP. Connaissances de base en sécurité informatique.

OBJECTIFS PEDAGOGIQUES

Identifier les composants et les fonctionnalités de base d'un firewall FortiGate. Expliquer les concepts de filtrage réseau et applicatif ainsi que les modes de fonctionnement du firewall. Configurer un firewall FortiGate pour mettre en œuvre une politique de filtrage réseau et applicatif. Analyser les besoins de sécurité d'une organisation et adapter les configurations du firewall en conséquence. Intégrer les fonctionnalités avancées telles que le VPN IPSEC et SSL dans une architecture de sécurité existante. Évaluer l'efficacité des configurations de sécurité mises en place et proposer des améliorations pour répondre aux besoins évolutifs de l'entreprise.

MOYENS PEDAGOGIQUES

Tour de table au début de chaque formation pour définir les objectifs de chaque participant,
Alternance entre apports théoriques (en moyenne 30%) et exercices pratiques (en moyenne 70%),
Utilisation de cas concrets issus de l'expérience professionnelle de nos formateurs,
Remise d'un support de cours,
Assistance post-formation d'une durée de 1 an sur le contenu de la formation via notre adresse mail dédiée formateurs@atp-formation.com

MOYENS PERMETTANT LE SUIVI DE L'EXECUTION ET DES RESULTATS

Positionnement préalable oral ou écrit,
Evaluation des acquis tout au long de la formation par des exercices de synthèse,
Attestation de stage remise à chaque apprenant, avec son niveau d'acquisition pour chaque objectif pédagogique,
Feuille de présence signée par demi-journée,
Questionnaire de satisfaction pour évaluer la qualité de l'enseignement,
En option : passage certification possible selon les thématiques.

MOYENS TECHNIQUES EN PRESENTIEL

Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs récents et performants, d'un vidéo projecteur et d'un tableau blanc.

MOYENS TECHNIQUES DES CLASSES A DISTANCE

Grâce à un logiciel comme Teams, suivez une formation en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur.
Nous vous conseillons très fortement l'utilisation de votre webcam et de disposer d'un double écran.
Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition par téléphone au 04.76.41.14.20.

ORGANISATION

Les cours ont lieu de 9h00-12h30 13h30-17h00 (adaptable à la demande).

PROFIL FORMATEUR

Nous recrutons méticuleusement nos formateurs selon 3 critères: expertise, pédagogie et agilité.

ACCESSIBILITE

Les personnes atteintes de handicap souhaitant suivre nos formations sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités d'organisation.

MISE A JOUR

26/07/2024

Plan de cours N° : 651
Durée : 4 jours (28h)

FORTINET
Installation et configuration d'un firewall FortiGate

Introduction
- Technologies et caractéristiques des firewalls
- L'architecture
  - La famille des produits FORTINET
- Les composants de l'Appliance
- Configuration et administration
- Les tâches d'administration
- Les modes CLI/GUI et FortiManager
- La procédure d'installation
- Prise en main de l'interface
- Travaux pratiques
  - Installer et configurer le firewall

Le filtrage réseau et le filtrage applicatif
- La politique de contrôle d'accès du firewall
  - Le filtrage des adresses et des ports
- Définir une politique de filtrage
  - Gestion des règles
- Le filtrage de contenu et détection de pattern
- Le filtrage URL
  - Les options avancées
- Les filtres anti-spam
  - Le contrôle du protocole SMTP
- Les fichiers attachés
  - Les profils de protection
  - L'antivirus
  - Le blocage par extension de fichiers
- Travaux pratiques
  - Mise en place d'une stratégie de filtrage réseau et applicative

Le NAT et le routage
- Les modes d'utilisation NAT/Route/Transparent
- Le routage statique et le routage dynamique
- Quelle politique de routage mettre en place ?
- Travaux pratiques
  - Mise en place d'une politique de routage
  - L'authentification avec l'AD ou Radius

Les VLAN et le Virtual Domains (VDOM)
- Rappels sur le concept de VLAN
  - Quand l'utiliser ?
- Administration et supervision
- Le routage InterVDOM
- Travaux pratiques
  - Installation et configuration de VLAN et VDOM

Le VPN avec IPSEC
- Rappels d'IPSEC
  - Le VPN IPSEC site à site
- Le mode interface et le mode tunnel
- Le VPN IPSEC client à site
- Le client "FortiClient"
  - L'authentification Xauth
- Les tunnels avec la clé prépartagée
- Travaux pratiques
  - Configurer un tunnel IPSEC

Le VPN avec SSL
- Rappels sur le protocole SSL
- Le mode Tunnel et le mode Portail
- Choisir le mode appoprié
- Travaux pratiques
  - Configuration de tunnel SSL mode portail et tunnel

Haute disponibilité
- Les concepts de haute disponibilité
- Le mode actif-passif/actif-actif
- Répondre au besoin de l'entreprise
- Travaux pratiques
  - Mise en place de la haute disponibilité FGCP actif/passif