Fortinet, sécurité réseaux

Cours Pratique de 4 jours - 28h
Réf : TIR - Prix 2024 : 2 790€ HT

Cette formation vous apprendra à déployer la solution de sécurité Fortinet pour protéger votre réseau d'entreprise. A l'issue, vous serez capable de l'installer et maîtriserez les éléments essentiels de sa configuration, parmi lesquels le filtrage applicatif, les VPN et la haute disponibilité.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Décrire les fonctionnalités du FortiGate

Installer et configurer le firewall

Mettre en oeuvre une stratégie de filtrage réseau et applicative

Mettre en oeuvre un VPN SSL et IPSEC

Mettre en œuvre la haute disponibilité des FortiGate

LE PROGRAMME

dernière mise à jour : 09/2018

1) Introduction

- Technologies et caractéristiques des firewalls.
- L'architecture. La famille des produits FORTINET.
- Les composants de l'Appliance.

2) 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.

3) 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.

4) 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.

PARTICIPANTS

Techniciens, administrateurs et ingénieurs systèmes/réseaux/sécurité.

PRÉREQUIS

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

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

5) 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.

6) 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.

7) Le VPN avec SSL

- Rappels sur le protocole SSL.
- Le mode Tunnel et le mode Portail.
- Choisir le mode approprié.

Travaux pratiques : Configuration de tunnel SSL mode portail et tunnel.

8) 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.

LES DATES

PARIS
2024 : 23 avr., 11 juin, 01 juil., 24 sept., 05 nov., 17 déc.