Fortigate Securité – Infrastructure
Badge niveau 1 Fortinet Certified Professional – Network Security

Cours Pratique de 5 jours - 35h
Réf : FNA - Prix 2024 : 4 040€ HT

Cette formation FortiGate sécurité et infrastructure vous apportera toutes les connaissances liées à la gestion unifiée des menaces (Unified Threath Management ou UTM) sur une même plateforme. La partie "sécurité" vous fournira les acquis sur les pratiques liées aux règles générales de gestion et de protection contre les malwares. La partie "infrastructure" permettra, quant à elle, la maîtrise des fonctions d'architectures avancées du FortiGate.

PARTICIPANTS
Ingénieurs/administrateurs et techniciens réseau et toute personne impliquée dans la conception d'architectures réseau et de sécurité basées sur les matériels FortiGate.

PRÉREQUIS
Connaissances de base en sécurité informatique ainsi que de bonnes connaissances de TCP/IP.

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.

OBJECTIFS PÉDAGOGIQUES

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

Déployer le mode de fonctionnement approprié à son réseau (proxy, flow, NGFW…)

Utiliser conjointement les interfaces graphique et CLI pour l'administration

Contrôler l'accès réseau aux réseaux configurés à l'aide de politiques de pare-feu

Appliquer la redirection de port, le Network Address Translation (NAT) source et le NAT destination

Authentifier les utilisateurs à l'aide de politiques de pare-feu

Comprendre les fonctions de chiffrement et les certificats

Déchiffrer le trafic sécurisé SSL/TLS afin de l'inspecter

Configurer des profils de sécurité pour neutraliser les menaces et les abus

Appliquer des techniques de contrôle des applications réseau

Utiliser des protocoles et des ports standard ou non standard

Lutter contre le piratage et le déni de service (DoS)

Collecter et interpréter les items collectés dans les journaux

Identifier les caractéristiques du tissu de sécurité Fortinet (Security Fabric)

Analyser une table de routage FortiGate

Acheminer les paquets à l'aide de routes statiques et de routes basées sur des règles

Déployer les multichemins à charge équilibrée

Diviser FortiGate en deux ou davantage d'appareils virtuels

Configurer des domaines virtuels (VDOM)

Comprendre les principes fondamentaux et les avantages de l'utilisation de ZTNA

Proposer un VPN SSL pour un accès sécurisé à votre réseau privé

Établir un tunnel VPN IPsec entre deux appareils FortiGate

Implémenter un VPN maillé ou partiellement redondant

Diagnostiquer les échanges IKE ayant échoués

Offrir un accès Single Sign-On (FSSO) aux services réseau en adossant l'accès à Microsoft Active Directory (AD)

Déployer des appareils FortiGate en cluster haute disponibilité

Améliorer la tolérance aux pannes et fournir des performances élevées

Déployer l'interface virtuelle SD-WAN

Mettre en œuvre une répartition dynamique des flux selon des performances mesurées sur les interfaces membres

MÉTHODES PÉDAGOGIQUES

Alternance équilibrée de présentations, d'ateliers et de mises en situation.

TRAVAUX PRATIQUES

Travaux pratiques individuels et en groupe, réflexion collective. Les exercices pratiques sont réalisés sur la version FortiOS prévue par la certification Fortinet.

CERTIFICATION

Ce cours est conçu pour les candidats qui souhaitent passer l'examen Fortinet NSE4 – FortiOS. Il est la première étape dans la démarche de la certification NSE 5 – FortiGate Network Security Professional, elle permet le passage d'un examen badge (core) qu'il faudra combiner avec un électif et le passage d'un second examen FortiManager (réf. FNB) ou FortiAnalyzer (réf.FND). L'obtention des deux examens permet la validation du certificat Fortinet NSE5.

LE PROGRAMME

dernière mise à jour : 01/2024

1) Sécurité - Introduction et réglages initiaux

- Fonctionnalités de haut niveau.
- Les décisions initiales.
- Administration de base.
- Maintenance de base.

2) Sécurité - Politique de pare-feu

- Configuration de politiques.
- Gestion des politiques.
- Meilleures pratiques et dépannage.

3) Sécurité - Network Address Translation

- Introduction.
- NAT adossé à la politique versus NAT central.
- Meilleures pratiques et dépannage.

4) Sécurité - Authentification par firewall

- Méthodes d'authentification de pare-feu.
- Groupes d'utilisateurs.
- Règles de pare-feu avec authentification.

5) Sécurité - Logging et monitoring

- Notions de base sur les journaux.
- Journalisation locale ou distante.
- Réglages de journalisation, recherche dans les journaux.
- Protection des données de journalisation.

6) Sécurité - Opérations de certificat

- Authentifier et sécuriser les données à l'aide de certificats.
- Inspecter les données chiffrées.

7) Sécurité - Filtrage web

- Modes d'inspection.
- Bases du filtrage web.
- Fonctionnalités supplémentaires de filtrage web basées proxy.
- Filtrage Vidéo.
- Meilleures pratiques et dépannage.

8) Sécurité - Contrôle des applications

- Bases du contrôle des applications.
- Configuration du contrôle des applications.
- Journalisation et surveillance des événements de contrôle des applications.

9) Sécurité - Antivirus

- Fondamentaux.
- Modes d'analyse.
- Configuration de l'antivirus.

10) Sécurité - Prévention des intrusions
- Le système de prévention des intrusions.
- Déni de service.

11) Sécurité - Tissu de sécurité (Security Fabric)
- Notion de tissu de sécurité.
- Déploiement.
- Étendre le tissu de sécurité.
- Système de notation du tissu de sécurité et vue de la topologie.

12) Infrastructure - Routage
- Routage sur FortiGate.
- Surveillance du routage et attributs de routage.
- Partage de charge à coût égal.
- Test Reverse Path Forwarding (RPF), lutte contre l'usurpation d'adresse.
- Sondes de santé des liens et bascule de routes.
- Diagnostics.

13) Infrastructure - Domaines virtuels
- Concepts VDOM.
- Administrateurs VDOM.
- Configuration des VDOM.
- Liens interVDOM.
- Meilleures pratiques et dépannage.

14) Infrastructure - Fortinet Single Sign-On
- Fonction et déploiement.
- FSSO avec Active Directory.
- Réglages et dépannage.

15) Infrastructure - Zero Trust Network Access (ZTNA)
- Introduction.
- Comparer ZTNA aux VPNs IPsec et SSL.

16) Infrastructure - VPN SSL
- Modes de déploiement.
- Configuration.
- Surveillance et dépannage.

17) Infrastructure - IPsec VPN
- Introduction.
- Configuration.
- Routage et règles de pare-feu.
- VPN redondants, VPN maillé.
- Surveillance, journalisation.

18) Infrastructure - Haute disponibilité
- Modes de fonctionnement actif/passif versus actif/actif.
- Synchronisation du cluster HA.
- Basculement HA.

19) Infrastructure - SD-WAN
- Motivation, répartition de flux dynamique.
- Implémentation.
- Sondes de performance.
- Règles SD-WAN.

20) Infrastructure - Diagnostics

- Généralités.
- Débogage de flux.
- Processeur et mémoire.
- Micrologiciel et matériel.

LES DATES

CLASSE À DISTANCE
2024 : 27 mai, 29 juil., 07 oct., 16 déc.

PARIS
2024 : 13 mai, 30 sept., 09 déc.