Fortigate administration

Le prix ne comprend pas le passage de la certification

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Domaine : Cybersécurité - sécurité informatique

Filière : Outils

Rubrique : Fortinet - Shibboleth

Éligible au CPF : Non

Action collective : Non

PRÉSENTATION

Objectifs & compétences

Prendre en main les fonctions UTM du Fortigate.
Prendre en main les fonctions avancées du Fortigate.

Public visé

administrateurs systèmes Réseaux

Pré-requis

Aucun

PROGRAMME

JOUR 1

Introduction sur Fortigate et les UTM
Présentation de Fortigate, ses fonctionnalités et son rôle en tant que Unified Threat Management (UTM) pour la sécurité réseau.

TP : Installation et configuration initiale de Fortigate. Familiarisation avec l'interface de gestion.

Gestion des logs et supervision
Explication de l'importance de la gestion des logs pour la détection d'incidents de sécurité et la supervision du réseau.
Présentation des outils de gestion des logs et de supervision disponibles sur Fortigate.

TP : Configuration de la collecte des logs sur Fortigate. Utilisation d'un outil de supervision pour analyser les logs et détecter des événements de sécurité.

Les règles firewall
Compréhension des règles firewall et de leur rôle dans le filtrage du trafic réseau.
Apprentissage de la configuration des règles firewall sur Fortigate.

TP : Création de règles firewall sur Fortigate pour autoriser ou bloquer certains types de trafic. Test des règles en simulant différentes situations.

JOUR 2

Les règles firewall avec authentification des utilisateurs
Exploration de l'authentification des utilisateurs à travers les règles firewall.
Découverte de l'utilisation des informations d'identification des utilisateurs pour renforcer la sécurité du réseau.

TP : Configuration de l'authentification des utilisateurs sur Fortigate. Création de règles firewall basées sur les informations d'identification des utilisateurs.

Le VPN SSL

Code de formation : NE226

€ Tarifs

Prix public : 3500 €

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
Le dispositif FNE-Formation.
L'OPCO (opérateurs de compétences) de votre entreprise.
France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
CPF -MonCompteFormation
Contactez nous pour plus d'information : contact@aston-institut.com

Lieux & Horaires

Durée : 35 heures

Délai d'accès : Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

Prochaines sessions

Consultez-nous pour les prochaines sessions.

Mise en œuvre d'un VPN SSL pour permettre l'accès sécurisé des utilisateurs nomades au réseau de l'entreprise.
Apprentissage de la configuration du VPN SSL sur Fortigate.

TP : Configuration d'un VPN SSL sur Fortigate pour permettre l'accès distant sécurisé. Connexion à distance à travers le VPN et vérification de la connectivité.

Introduction au VPN IPSEC
Présentation du VPN IPSEC et de ses avantages pour les connexions sécurisées entre les sites distants.
Compréhension de la configuration du VPN IPSEC sur Fortigate.

TP : Configuration d'un VPN IPSEC entre deux sites distants à l'aide de Fortigate. Test de la connectivité entre les deux sites via le VPN.

JOUR 3

L'antivirus
Explication du rôle de l'antivirus dans la protection contre les logiciels malveillants.
Découverte des fonctionnalités antivirus disponibles sur Fortigate et apprentissage de leur configuration.

TP : Configuration de l'antivirus sur Fortigate. Simulation d'une attaque de logiciel malveillant pour vérifier l'efficacité de l'antivirus.

Le proxy explicite
Présentation du proxy explicite et de son rôle dans le filtrage du trafic Web.
Apprentissage de la configuration du proxy explicite sur Fortigate.

TP : Configuration du proxy explicite sur Fortigate. Utilisation du proxy pour filtrer le trafic Web et bloquer l'accès à certains sites.

Le filtrage d'URL
Mise en œuvre du filtrage d'URL en utilisant le proxy explicite, le cache et l'authentification des utilisateurs.
Exploration des fonctionnalités de filtrage d'URL disponibles sur Fortigate et apprentissage de leur configuration.

TP : Mise en œuvre du filtrage d'URL en utilisant le proxy explicite, le cache et l'authentification des utilisateurs. Test de l'accès à différentes catégories de sites Web.

Le contrôle applicatif
Compréhension du contrôle applicatif pour surveiller et limiter l'utilisation des applications au sein du réseau.
Apprentissage de la configuration du contrôle applicatif sur Fortigate.

TP : Configuration du contrôle applicatif sur Fortigate pour limiter l'utilisation de certaines applications. Test de l'utilisation des applications et vérification de l'application des politiques de contrôle.

JOUR 4

Le routage
Introduction aux concepts de routage et à la configuration du routage sur Fortigate.
Apprentissage des différentes méthodes de routage et de leur utilisation.

TP : Configuration du routage statique sur Fortigate en interconnectant plusieurs réseaux. Vérification de la connectivité entre les réseaux en utilisant des outils de diagnostic.

La virtualisation
Compréhension de la virtualisation sur Fortigate.
Configuration des interfaces virtuelles, des VDOM (Virtual Domains) et des VLANs pour optimiser la segmentation du réseau.

TP : Création d'un VDOM (Virtual Domain) sur Fortigate et configuration d'interfaces virtuelles. Segmentation du trafic en attribuant différentes interfaces virtuelles à des zones spécifiques.

Le mode transparent
Explication du mode transparent sur Fortigate et de son utilisation dans des scénarios spécifiques.
Configuration du mode transparent et comparaison avec le mode routé.

TP : Configuration du mode transparent sur Fortigate entre deux segments de réseau. Vérification du fonctionnement du mode transparent en analysant le trafic réseau.

La haute disponibilité
Présentation des fonctionnalités de haute disponibilité sur Fortigate pour assurer la continuité des services.
Configuration de la haute disponibilité active-passive ou active-active.

TP : Configuration d'un cluster en haute disponibilité sur Fortigate avec un mode actif-passif. Simulation d'une défaillance du nœud actif pour tester la transition vers le nœud passif.

Le VPN IPSec avancé
Approfondissement du VPN IPSec et de ses fonctionnalités avancées sur Fortigate.
Configuration de tunnels VPN avec des options de sécurité avancées telles que la prévention de l'intrusion.

TP : Configuration d'un VPN IPSec sur Fortigate avec des fonctionnalités avancées telles que la prévention de l'intrusion et le contrôle d'accès. Vérification de la connectivité sécurisée entre les sites distants.

L'IPS (Intrusion Prevention System)
Introduction à l'IPS sur Fortigate pour détecter et prévenir les attaques réseau.
Configuration des règles d'IPS et analyse des journaux d'incidents.

TP : Activation de l'IPS sur Fortigate et configuration de règles pour détecter et prévenir les attaques courantes. Simulation d'attaques pour vérifier l'efficacité de l'IPS.

JOUR 5

Le FSSO (Fortinet Single Sign-On)
Explication du FSSO et de son utilisation pour l'authentification unique sur Fortigate.
Configuration du FSSO pour intégrer Fortigate avec des services d'annuaire.

TP : Configuration de l'intégration du FSSO avec un service d'annuaire tel que Active Directory. Authentification des utilisateurs sur Fortigate via le FSSO et vérification de l'accès aux ressources.

Les certificats, la cryptographie
Présentation des certificats et de la cryptographie sur Fortigate pour sécuriser les communications.
Génération de certificats et configuration de la gestion des certificats sur Fortigate.

TP : Génération de certificats sur Fortigate et configuration de la gestion des certificats. Configuration de l'authentification basée sur des certificats et test de la connexion sécurisée.

Le DLP (Data Loss Prevention)
Introduction au DLP sur Fortigate pour protéger les données sensibles contre les fuites.
Configuration des règles de DLP et test des politiques de prévention de la perte de données.

TP : Génération de certificats sur Fortigate et configuration de la gestion des certificats. Configuration de l'authentification basée sur des certificats et test de la connexion sécurisée.

Les diagnostics
Utilisation des outils de diagnostic sur Fortigate pour résoudre les problèmes de connectivité et de performances réseau.
Analyse des journaux, utilisation des commandes de diagnostic et interprétation des résultats.

TP : Configuration de règles de DLP sur Fortigate pour détecter et prévenir les fuites de données sensibles. Envoi de données sensibles pour tester les politiques de prévention de la perte de données.

L'accélération matérielle
Présentation de l'accélération matérielle sur Fortigate pour améliorer les performances du pare-feu.
Configuration des options d'accélération matérielle et mesure des gains de performances.

TP : Activation de l'accélération matérielle sur Fortigate et mesure des performances avant et après l'activation. Comparaison des performances

avec et sans accélération matérielle.

IPv6
Introduction à IPv6 et à son déploiement sur Fortigate.
Configuration de la prise en charge IPv6, la translation d'adresse (NAT) et l'inspection du trafic IPv6.

TP : Configuration de la prise en charge IPv6 sur Fortigate, y compris la configuration de l'adressage IPv6, de la translation d'adresse (NAT) et de l'inspection du trafic IPv6. Vérification de la connectivité IPv6.

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.
Pédagogie : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.
Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.
Pendant la formation : mises en situation, autodiagnostics, travail individuel ou en sous-groupe sur des cas réels.

Méthode

Fin de formation : entretien individuel.
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.
Assiduité : certificat de réalisation.
Validations des acquis : grille d'evalution des acquis établie par le formateur en fin de formation.