Formation CNSA - Certified Stormshield Network Administrator

Durée :	3.0 jour(s)
Objectifs :	• Prendre en main un firewall SNS et connaître son fonctionnement • Configurer un firewall **Stormshield** dans un réseau • Définir et mettre en oeuvre des politiques de filtrage et de routage • Mettre en place différents types de réseaux privés virtuels (VPN IPSec et VPN SSL)
Public :	• Responsables informatiques, Administrateurs réseaux, Techniciens informatiques
Prérequis :	• Avoir de bonnes connaissances TCP/IP, une formation réseau préalable est un plus • Il est demandé aux stagiaires souhaitant s'inscrire en formation CSNA de valider au préalable qu'ils disposent des connaissances nécessaires pour participer à la formation grâce au test d'autoévaluation au lien suivant : test d'auto-évaluation CSNA.
Modalités et moyens pédagogiques	La formation alterne cours théorique et travaux pratiques. Deux modalités sont proposées : • en présentiel, dans les locaux de Stormshield • en distanciel, avec présence à distance du formateur grâce à un système de visio et du portail web: maformation.vaelia.fr
Modalités d'évaluation	• Auto évaluation des acquis, exercices pratiques et/ou échanges avec le formateur. • Deux passages de certification CSNA permettent aux stagiaires de valider leurs acquis.
Moyens d'encadrement	Un formateur expert spécialisé en Stormshield Network Security dont les compétences ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou Vaelia.
Satisfaction globale :	/5 *Calculée à partir des évaluations stagiaires sur les 12 derniers mois.*

Jour 1

Prise en main du firewall

- Enregistrement sur l'espace client et accès aux ressources techniques
- Initialisation du boitier et présentation de l'interface d'administration
- Configuration système et droits d'administration
- Installation de la licence et mise à jour de la version du système
- Sauvegarde et restauration d'une configuration

Traces et supervisions

- Présentation des catégories de traces
- Supervision et graphiques d'historiques

Les objets

- Notion d'objet et types d'objets utilisables
- Objets réseau et routeur

Jour 2

Configuration réseau

- Modes de configuration d'un boitier dans un réseau
- Types d'interfaces (Ethernet, modem, bridge, VLAN, GRETAP)
- Types de routage et priorités

Translation d'adresses (NAT)

- Translation sur flux sortant (déguisement)
- Translation sur flux entrant (redirection)
- Translation bidirectionnelle (translation un pour un)

Filtrage

- Généralités sur le filtrage et notion de suivi de connexion (stateful)
- Présentation détaillée des paramètres d'une règle de filtrage
- Ordonnancement des règles de filtrage et de translation

Protection applicative

- Mise en place du filtrage URL en http et https
- Configuration de l'analyse antivirale et de l'analyse par détonation Breach Fighter
- Module de prévention d'intrusion et profils d'inspection de sécurité

Jour 3

Utilisateurs et authentification

- Configuration des annuaires
- Présentation des différentes méthodes d'authentification (LDAP, Kerberos, Radius, Certificat SSL, SPNEGO, SSO)
- Enrôlement d'utilisateurs
- Mise en place d'une authentification explicite via portail captif

Les réseaux privés virtuels

- Concepts et généralités VPN IPSec (IKEv1 et IKEv2)
- Site à site avec clé pré-partagée
- Virtual Tunneling Interface

VPN SSL

- Principe de fonctionnement
- Configuration