+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 11/07/2024

S'inscrire

Formation et préparation à la Certification Stormshield© Network Administrateur (EDU-CSNA)

ALL-IN-ONE : EXAMEN INCLUS AU TARIF AVEC LE COURS STORMSHIELD© NETWORK ADMINISTRATEUR

3 jours (21 heures)

PRÉSENTATION

La certification Stormshield© Network Administrateur (CSNA) atteste de vos compétences fondamentales en gestion et sécurisation des réseaux avec les solutions Stormshield.

Avec notre formation et notre programme, vous développerez des compétences pratiques et théoriques essentielles, visant à renforcer votre expertise dans la configuration, la gestion, la supervision, et la sécurisation des réseaux avec les firewalls Stormshield.

Notre formation couvre des aspects cruciaux tels que la prise en main du firewall, la configuration réseau, la translation d'adresses, le filtrage, la protection applicative, l'authentification des utilisateurs, et les réseaux privés virtuels (VPN). Avec un équilibre parfait entre théorie approfondie et travaux pratiques, ce cours vous offre une préparation complète dans les disciplines essentielles de l'utilisation des solutions StormShield.

Chaque module met à l'épreuve vos connaissances et compétences dans des domaines spécifiques de la gestion et de la sécurisation des réseaux.

La formation est constamment mise à jour pour refléter les dernières tendances et évolutions dans le domaine de la cybersécurité et de la gestion des réseaux.

OBJECTIFS

- Comprendre les concepts de base des firewalls Stormshield et leur architecture
- Apprendre à configurer et administrer un firewall Stormshield
- Superviser et analyser les traces et les graphiques d'historiques

- Gérer les objets réseau et les configurations réseau avancées
- Mettre en œuvre des stratégies de translation d’adresses (NAT) et de filtrage
- Configurer des protections applicatives
- Administrer les utilisateurs et les méthodes d'authentification
- Implémenter et gérer des VPN IPSec et SSL

PUBLIC VISÉ

- Administrateurs de réseaux
- Ingénieurs de sécurité
- Responsables informatiques
- Consultants en cybersécurité
- Architectes réseaux

Pré-requis

- Connaissance de base en administration de réseaux et en sécurité informatique
- Expérience pratique avec les firewalls ou les solutions de sécurité réseau
- Connaissances de base en TCP/IP et en routage réseau

Pré-requis techniques

- Accès à un firewall Stormshield pour les travaux pratiques
- Un ordinateur capable de faire fonctionner des outils de gestion de réseau
- Navigateurs web compatibles pour accéder à l’interface Stormshield
- Connexion Internet stable

PROGRAMME DE NOTRE FORMATION STORMSHIELD© NETWORK ADMINISTRATEUR

JOUR 1 :

PRISE EN MAIN DU FIREWALL

- Enregistrement sur l'espace client et accès aux ressources techniques
- Initialisation du boîtier 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

Configuration Réseau

- Modes de configuration d'un boîtier dans un réseau
- Types d'interfaces
- Ethernet
- Modem
- Pont
- VLAN
- GRETAP
- Types de routage et prioritaires

JOUR 2 :

Translation d’adresses (NAT)

- Sur flux sortant
- Sur flux entrant (redirection)
- 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 traduction

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
- RAYON
- Certificat SSL
- SPNEGO
- authentification unique
- Enrôlement d'utilisateurs
- Mise en place d'une authentification explicite via portail captif

Les réseaux privés virtuels

- Concepts et généralités VPN IPSec (IKEv1 IKEv2)
- Site à site avec clé pré-partagée
- Interface de tunneling virtuel

VPN SSL

- Principe de fonctionnement
- Configuration

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.