Certified Stormshield Network Troubleshooting and Support (NT-CSNTS)

Durée: 4 Jours **Réf de cours: NT-CSNTS** **Méthodes d'apprentissage: Intra-entreprise & sur-mesure**

Résumé:

Maîtrisez toutes les subtilités du dépannage et du support réseau

Ce cours a pour but d'exposer des outils et méthodes pour collecter les informations nécessaires à l'étude et à la correction de problèmes en utilisant l'interface en ligne de commande (CLI) des firewalls Stormshield Network Security.
Grâce à cette formation certifiante, devenez la référence technique des firewalls Stormshield Network Security au sein de votre entreprise.
Vous étudiez dans cette formation les fonctionnalités avancées des produits Stormshield Network Security au sein d'une architecture complexe.
Durant la formation Certified Stormshield Network Troubleshooting and Support (CSNTS), vous prenez en main les fonctionnalités les plus avancées des firewalls Stormshield Network Security.

Mis à jour 28/05/2026

Formation intra-entreprise

Cette formation est délivrable en session intra-entreprise, dans vos locaux ou dans les nôtres. Son contenu peut être adapté sur-mesure pour répondre aux besoins de vos collaborateurs. Contactez votre conseiller formation Global Knowledge ou adressez votre demande à info@globalknowledge.fr.

Public visé:

Responsables informatique, administrateurs rseau, tout technicien informatique.

Objectifs pédagogiques:

- A l'issue de la formation, et après une révision des connaissances de base, les participants seront capables de :
- Comprendre l'organisation du système de fichiers ainsi que les démonstrations et processus d'une appliance Stormshield Network.
- Localiser, explorer et manipuler les différents fichiers de configuration et de journalisation des activités (logs).
- Distinguer des particularités et anomalies dans une configuration réseau et routage.
- Réaliser et d'étudier des captures de trafic réseau.
- Étudier une politique de sécurité et d'en identifier les directives générales et les paramètres particuliers.
- Identifier les traitements appliqués aux connexions en cours.
- Produire un relevé d'informations adapté, complet et exploitable pour l'établissement d'un diagnostic.
- Configurer des politiques de tunnels VPN IPSec, d'identifier les mécanismes activés et d'en diagnostiquer les dysfonctionnements.
- Analyser et de diagnostiquer une configuration en haute disponibilité.

Pré-requis:

Les participants doivent avoir une certification CSNE en cours de validité.

- Connaissances approfondies en TCP/IP et shell UNIX.

Les prérequis matériels dépendent du format de la session.

En présentiel :

Test et certification

La certification CSNTS consiste en un examen effectué en ligne (3h, 60 questions).

L'examen comporte des QCM et des questions ouvertes sur les fonctionnalités, paramétrages et méthodes de dépannage avancées à mettre en œuvre pour répondre exhaustivement à des rapports d'incidents issus de clients.

- PC portable avec une interface réseau filaire et avec un système d'exploitation Windows de préférence (physique ou virtuel en accès réseau par pont) avec droits d'administrateur ; et disposant des logiciels suivants : Firefox, PuTTY (ou tout autre client SSH), WinSCP (ou client SCP équivalent), Wireshark, VirtualBox ou équivalent VMWare (VMWare Workstation Player ou Pro).

En distanciel :

- Navigateur web, en dernière version : Chrome ou Firefox avec Javascript installé (seuls ces navigateurs sont supportés)
- Vérification de l'accès à la plateforme CyberRange (https://customers.cyberrange.cloud/) avant la formation
- Droits d'installation pour le logiciel de visio
- Accès internet avec un débit minimal de 2Mb/s
- Une webcam et un micro fonctionnels
- Un 2ème écran est fortement recommandé (22'' ou plus)

Le score minimum de certification est de 70%.

L'examen est ouvert automatiquement le jour suivant la fin de la formation pour une durée de six mois sur la plateforme https://institute.stormshield.eu .

En cas d'échec ou d'impossibilité de passer l'examen dans ce créneau, un deuxième et dernier passage d'examen est ouvert automatiquement dans la foulée pour une durée d'une semaine.

Contenu:

Introduction

Système d'exploitation et commandes UNIX liées

- Méthodes d'accès au shell et paramètres
- SSH : fonctionnalités
- Système de fichier et commandes associées
- Répertoires et commandes associées
- Environnement système et utilisateur
- Fichiers et commandes associées

Logs

- Logs locaux : localisation, caractéristiques, syntaxe, catégories
- Commandes associées
- Fichiers de configuration
- Logd, logctl, journalisation des messages noyau
- Fichiers de configuration
- Répertoires, structure et syntaxe générale
- Sauvegarde (*.na), decbackup, tar
- Configuration usine

Objets

- Syntaxe des objets
- Objets dynamiques et FQDN

Réseau et routage

- Paramètres des interfaces réseau
- Le bridge et les commandes associées
- Routage : fonctions de routage et leur priorité
- Routes par défaut et routes statiques
- Gatemon et les objets routeurs
- Routage dynamique
- Commandes relatives, affichage des routes
- Mode verbose
- LAB Réseau et routage

Capture et analyse de trafic

- Introduction et conseils
- Syntaxe générale et arguments
- Filtres usuels
- Exemples commentés et préparation pour faire de bonnes captures
- Analyse de trafics par tcpdump (flux TCP, UDP/icmp)
- LAB network/tcpdump

ASQ : les étapes d'analyse

- Analyse pas à pas des couches réseau
- Commandes associées
- Paramètres globaux
- Profils et paramètres particuliers
- ASQ asynchrone : différents cas et watermarking
- ASQ verbose mode
- LAB paramètres ASQ

ASQ : politique de sécurité

- Répertoires et fichiers de configuration, syntaxe des règles
- Filtre : commandes associées
- Filtre : exemple de règles chargées (action, niveau d'inspection, plugin, PBR,
- QoS, interfaces, proxy)
- Filtre : traduction des groupes et des listes
- NAT : rappels (NAT Dynamique, NAT Statique par port, NAT statique/Bimap,
- Non NAT)
- NAT : commandes associées
- NAT : syntaxe des règles chargées
- LAB NAT et Filtrage

ASQ : Stateful et tables d'états

- Table des adresses protégées
- Table des hôtes
- Table des connexions : exemples d'états de connexion (NAT, vconn, FTP
- plugin, async, lite...)
- LAB ASQ Stateful tracking

Démons et Processus

- Liste et rôle
- Démon Superviseur
- Commandes relatives

Eventd : le gestionnaire d'événements

VPN IPSec

- Implémentation IKE/IPSec Stormshield Network
- Fichiers de configuration
- Politique de sécurité (SPD, SAD)
- Les négociations IKE
- Négociations : mode Main et mode Aggressive
- ISAKMP et IPsec SA
- Propositions IKE
- Particularités : NAT-T, DPD, Keepalive, SharedSA, Politique None, SPD Cache
- Commandes associées
- Analyse d'une IPSec-SA
- Logs
- Notifications de « delete SA »
- Capture et analyse du trafic ISAKMP
- Particularités des correspondants dynamiques
- Mode Verbose, erreurs courantes
- LAB ISAKMP/IPsec

PKI et certificats

- Rappels et directives globales
- Répertoire de CA
- Astuces de configuration
- Vérification des certificats

Haute disponibilité

- Généralités
- Fichiers de configuration
- Commandes relatives
- Etapes d'activation, gestion des interfaces réseau
- Processus et trafics impliqués
- Réplications/synchronisation
- Evènements et logs HA

Méthodes pédagogiques :

La formation est délivrée soit en présentiel (en face à face pédagogique en salle), soit en distanciel (présence à distance du formateur grâce à un système de visio et utilisation de la plateforme CyberRange d'Airbus). La formation alterne cours théorique et travaux pratiques.
Les participants reçoivent un support de cours composé du cours, des travaux pratiques (Labs) et de leurs corrections. Afin de pouvoir mettre en pratique les éléments du cours, les stagiaires ont à leur disposition un environnement technique complet.
Afin de maintenir l'expertise des participants, toutes les mises à jour du support de cours sont accessibles au format PDF durant 3 ans sur la plateforme https://institute.stormshield.eu .
Ils trouveront également sur cette plateforme un environnement virtuel permettant de manipuler le produit et rejouer les Labs en toute autonomie.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement