Certified SonicWall Security Professional (CSSP)

Public visé

Ingénieurs système, distributeurs, intégrateurs, utilisateurs finaux

Cette formation peut faire l'objet d'une demande de prise en charge au titre de la formation continue auprès de votre OPCA. **no. d'agrément D2B: 11 93 05082 93.**

Pré-requis

- Une certification SNSA active dans SonicOS.

Des connaissances et une expérience dans le domaine du réseau :

- Connaissance approfondie des concepts de réseau, des topologies de réseau et du modèle OSI des piles de protocoles réseau
- Compréhension du TCP / IP, de l'adressage réseau, des sous-réseaux et de la traduction d'adresses réseau (NAT)
- Connaissance des concepts de routage
- Connaissance de la fonctionnalité et de la mise en œuvre d'IPSec

e-Learning :

- Advanced Network Security (environ 4 heures de course en ligne) : Le programme d'e-Learning "Advanced Network Security" en cinq modules, est une condition préalable à la formation NSAA. Cette formation autodidacte explique comment exploiter des technologies de sécurité uniques, telles que le routage dynamique, la VoIP, la QoS, la SSL et l'Intelligence Artificielle, sur les pare-feu afin d'améliorer leur efficacité, leurs performances et leur évolutivité. Les modules fournissent une compréhension conceptuelle de ces technologies de sécurité et de réseau avancées afin de mettre en place des stratégies et des mesures d'assainissement, y compris les configuration, d'implémentation et de dépannage spécifiques à SonicWall.

Objectifs

A l'issue de cette formation l'apprenant sera capable de :

- Utiliser les fonctionnalités avancées de Sonicwall
- Déployer de la haute disponibilité
- Gérer le routage OSPF
- Gérer la VOIP via le Sonicwall
- Gérer le mode filaire
- Surveiller et optimiser le réseau
- Mettre en place et gérer le contrôle d'application

Contenu de la formation

Section 1 : Introduction au cours

- Introduction au cours

Section 2 : Outil de dépannage du SonicOS

- Vue d'ensemble du dépannage
- Sauvegarde et restauration du système
- Outils de diagnostic
- Capture de paquets
- Logs
- Outils tiers

Section 3 : Réseau avancé

- Routage avancé
- RF-DPI
- DPI-SSL

Section 4 : Surveillance et optimisation du réseau

- Intelligence d'application
- Contrôle d'application

- Gestion de la bande passante
- Content Filtering Services via App Rules
- Expressions régulières

Section 5 : Rapports Appflow et mode filaire

- Rapports Appflow
- Vue d'ensemble de GMS
- Mode filaire
    - Tap Deployment
    - Inline Deployments

Section 6 : SIP

- Vue d'ensemble de la VOIP
- Transformation SIP

Section 7 : Déploiement de la Haute Disponibilité

- Haute Disponibilité avancée
- Actif/Passive vs Actif/Actif
- Cluster A/A
- Configuration Haute Disponibilité

Moyens et méthodes pédagogiques

La formation se déroule avec une alternance d'exposés ou de présentations, de travaux pratiques/dirigés et de quiz.

Chaque participant a accès à un PC et un boitier Sonicwall pour la mise en pratique des notions abordées.

Un support de cours (essentiellement en anglais) est fourni sous format papier à chaque participant.

Les compétences acquises sont vérifiées au travers de mises en situation et/ou de quiz.

Durée : 14 heures sur 2 jours

Formateur : Qualification et compétences

La formation est assurée par Aslan ZELLI qui travaille depuis plus de 20 ans dans le domaine des réseaux informatiques, dont plus de 10 ans à utiliser, configurer et administrer des solutions SonicWall. Aslan ZELLI est CST (Certified SonicWall Trainer).

Taille du groupe de participants

Afin d'assurer un parfait suivi des participants et une grande interactivité entre le formateur et les apprenants chaque session ne dépassera pas 8 personnes.

Suivi des participants

L'assiduité des participants est attestée par la signature pour chaque ½ journée d'une feuille de présence par le participant et le formateur.

Evaluation de la formation

L'évaluation de la formation se fait à chaud par un questionnaire de satisfaction ainsi que des échanges directs entre le formateur et les participants.

Les points principaux à évaluer portent sur la qualité pédagogique du formateur, la qualité et le contenu du support de cours ainsi que la qualité de l'infrastructure utilisée.

Une partie du questionnaire portera également sur l'atteinte des objectifs initiaux du participant et sur ses souhaits en matière de formations complémentaires.

L'examen de certification est disponible en ligne via votre compte personnel MySonicWall. Vous recevrez une clé d'activation à l'issue du cours qui vous permettra d'accéder à l'examen (3 essais sont possibles). Tout participant qui réussit ce cours et passe l'examen de certification sera considéré comme Certified SonicWall Security Professional (CSSP).

Pour l'examen, 180 minutes sont allouées pour 60 questions. Un score de minimum 80% est requis pour réussir la certification. L'examen couvre tout le matériel de cours, y compris le contenu e-Learning. L'examen ne se limite pas aux documents couverts en classe et peut inclure le matériel trouvé dans les guides de l'administrateur SonicOS ou les articles de la base de connaissances.

À la fin de l'examen, vous êtes immédiatement informé de votre score d'examen et si vous avez réussi ou a échoué l'examen. Après avoir passé avec succès l'examen, vous recevrez un courrier électronique contenant votre certificat CSSP.

Durée de la certification : toutes les certifications SonicWall sont valides pendant deux ans à partir de la date à laquelle vous passez l'examen.