Programme Technique

Formation Certifiante Hillstone HCSA

Votre première étape vers l'expertise en cybersécurité. La certification **Hillstone Certified Security Associate (HCSA)** permet aux professionnels débutants et juniors de développer leurs compétences en déploiement et administration des pare-feux nouvelle génération **Hillstone Networks.**

Présentation de la formation

Dans un environnement de cybersécurité en constante évolution, la certification **HCSA** constitue une première étape pour acquérir les compétences fondamentales nécessaires au déploiement et à l'administration d'un **Next-Generation Firewall (NGFW)**.

La formation couvre les principales fonctionnalités de sécurité réseau de Hillstone Networks ainsi que des concepts modernes tels que le **Zero Trust** et les opérations de sécurité assistées par l'intelligence artificielle.

La formation combine les connaissances théoriques avec des **travaux pratiques (LAB)** permettant aux participants de mettre directement en application les notions étudiées.

Durée : 3 jours en présentiel | **Horaires :** 08h30 – 17h30

Public concerné	**Les bénéfices**
• Ingénieurs juniors et techniciens informatiques. • Personnel chargé du support informatique. • Administrateurs systèmes et réseaux. • Étudiants en réseaux ou cybersécurité. • Partenaires et clients Hillstone Networks souhaitant acquérir les compétences fondamentales.	• Obtenir une certification reconnue par le constructeur. • Développer des compétences pratiques sur les fonctionnalités essentielles d'un NGFW. • Comprendre les fondamentaux de la protection des réseaux. • Découvrir les principes du Zero Trust et de la prévention des menaces. • Se préparer à l'examen de certification HCSA.

JOUR 01

Chapitres 1 à 3 — Fondamentaux, gestion système et architecture

08h30 – 10h00	**Chapitre 1 — Introduction au NGFW** • Introduction au Next-Generation Firewall (NGFW) • Cybersécurité intégrative • Évolution des technologies d'attaque et de défense • Présentation et fonctions du Hillstone NGFW • Introduction au Zero Trust • Introduction aux opérations de sécurité assistées par l'IA
10h00 – 12h00	**Chapitre 2 — Gestion du système** • Gestion système par défaut • Gestion des licences • Mise à niveau du firmware • Gestion des équipements • Administration du système
12h30 – 14h00	■ **Pause déjeuner**
14h15 – 15h45	**Chapitre 3 — Architecture et modes de déploiement** • Architecture du système StoneOS • Modes de déploiement réseau • Intégration du NGFW dans l'infrastructure réseau

15h45 – 17h00	**Chapitre 3 — Technologies de routage** Présentation des technologies de routage et des principes nécessaires au déploiement et au fonctionnement du NGFW.

JOUR 02

Chapitres 4 à 7 — Politiques de sécurité, NAT, VPN et prévention des intrusions

08h30 – 10h30	**Chapitre 4 — Politiques de sécurité** • Concepts des politiques de sécurité • Objets de sécurité • Création et gestion des politiques • Contrôle des flux réseau • Options avancées des politiques
10h30 – 12h00	**Chapitre 5 — Network Address Translation (NAT)** • Concept du NAT • Configuration SNAT • Configuration DNAT • Options avancées du NAT
12h30 – 14h00	■ **Pause déjeuner**
14h15 – 15h45	**Chapitre 6 — VPN IPSec & SSL VPN** • Concept du VPN IPSec • Configuration du VPN IPSec • Concept du VPN SSL • Configuration du VPN SSL
15h45 – 17h00	**Chapitre 7 — Pratique de prévention des intrusions** • Enjeux actuels liés aux cybermenaces • Principes de prévention des intrusions • Configuration et fonctionnement de l'IPS • Protection Antivirus • Prévention des communications Botnet C&C;

JOUR 03

LAB pratiques — Mise en application opérationnelle

08h30 – 09h00	**Révision et briefing LAB** Rappel des notions clés des chapitres 1 à 7 et présentation des différents scénarios pratiques.
09h00 – 10h30	**LAB 01 — Gestion du système** • Administration du système • Gestion des licences • Opérations de gestion de l'équipement
10h30 – 12h00	**LAB 02 — Architecture, déploiement et routage** • Configuration des interfaces • Modes de déploiement • Mise en œuvre du routage
12h30 – 14h00	■ **Pause déjeuner**

14h00 – 15h00	**LAB 03 — Politiques de sécurité et NAT** • Création des objets • Configuration des politiques de sécurité • Contrôle des flux • Configuration SNAT • Configuration DNAT
15h00 – 16h00	**LAB 04 — IPSec VPN & SSL VPN** • Mise en œuvre d'un scénario VPN IPSec • Mise en œuvre d'un scénario SSL VPN • Vérification des connexions sécurisées
16H00 – 17h00	**LAB 05 — Prévention des menaces** • Configuration IPS • Protection Antivirus • Prévention Botnet C&C; • Analyse des résultats
17h00 – 17h30	**Évaluation, révision HCSA & clôture** Synthèse des compétences acquises, questions-réponses, révision des points clés et préparation à l'examen HCSA.

Examen de certification HCSA

À l'issue de la formation, les participants sont préparés à l'examen de certification **Hillstone Certified Security Associate (HCSA)**.

• **Format :** questions à choix multiples (QCM).
• **Durée :** 90 minutes.
• **Objectif :** évaluer les connaissances fondamentales nécessaires au déploiement et à l'administration d'un NGFW Hillstone.

HAFS NETWORKS ACADEMY
Authorized Training Center (ATC)

Centre de formation dédié aux technologies de cybersécurité, aux pare-feux nouvelle génération et aux solutions **Hillstone Networks.**