



## CISCO CCNA SECURITE

### Contexte & Objectifs de la formation

**Cisco** est le leader mondial dans les réseaux informatiques, son offre de produits et services s'étend de la PME à la multinationale, en passant par les cœurs de réseaux Internet des fournisseurs d'accès.

Les formations **Cisco** permettent une approche pragmatique aussi bien sur les standards Mondiaux que sur les technologies propriétaires de la marque. Cette mixité et la grande partie consacrée à la pratique fournissent des compétences solides pour les métiers liés aux réseaux.

### **Objectif de la formation:**

- Permettre aux participants de maîtriser la sé-curité des réseaux informatiques en environnement professionnel d'une part et d'obtenir la certification CCNA Security 210-260 d'autre part.
- Les compétences acquises à l'obtention de ce titre de certification Cisco valident les compétences dans l'installation, la maintenance et la surveillance des technologies et équipements de sécurité Cisco. Les professionnels certifiés CCNA Security auront la capacité de développer des politiques de sécurité et de limiter les risques au sein du système d'information.

### **PRÉPARATION À L'EXAMEN :**

- Les participants suivront un coaching sous la supervision du formateur sans frais supplémentaires. Nous garantissons un taux de 100% de réussite pour les participants assidus respectant nos recommandations.

### **Avantage pour les étudiants:**

- Accéder à des postes de haute responsabilité dans les meilleurs entreprises algériennes et internationales
- Occuper des emplois fortement rémunérés
- Progresser au sein de sa carrière

### **CONDITIONS D'ACCÈS :**

Posséder la certification CCENT ou CCNA R&S.

### Déroulement de la formation

- La formation se donnera selon les normes des académies Cisco, Le curriculum de cours sera mis à la disposition de chaque étudiant sur support électronique, un atelier équipé avec du matériel Cisco sera aussi mis à leur disposition.
- Chaque étudiant aura un compte Internet dans l'académie Cisco, lui permettant de télécharger les outils nécessaires au cours tels que le curriculum, les laboratoires, les simulateurs, les études de cas, les évaluation, etc.
- La formation peut être organisée en cours du jour de samedi à jeudi de 08h30' à 15h30' ou en cours du soir de 17h à 20h selon la demande

### **LA CERTIFICATION CCNA SÉCURITÉ :**

Le programme CCNA Sécurité est composé d'un seul cours de onze chapitres

### **Population concernée:**

La certification **CCNA Sécurité (Cisco Certified Network Associate)** est destinée aux spécialiste en sécurité réseaux, aux administrateurs et ingénieurs support intervenant dans la **sécurité réseaux**.

## FRAIS DE FORMATION

Le paiement des frais de formation s'effectue au début du cours.

### Durée de la formation

**80h**

### Dossier d'Inscription

- Une (01) Copie de la pièce d'Identité
- Une (01) Photo d'identité

# INSIM



**Business School**

Renseignement et Inscription

Ecole de Formation Professionnelle  
INSIM

Siège :  
02, rue Petite Provence Sidi Yahia  
Hydra Alger

Tél & Fax :  
021 69 44 33 / 021 43 59 86  
Site Web : [insim.dz](http://insim.dz)  
[cisco@insim.dz](mailto:cisco@insim.dz)

# PROGRAMME

## Chapitre 1: Les menaces de sécurité des réseaux modernes

Objectif: Expliquer les menaces à la sécurité des infrastructures réseaux modernes et leur atténuation

## Chapitre 2: Sécurisation des périphériques réseau

Objectif: sécuriser les routeurs Cisco.

## Chapitre 3: Authentification, autorisation et comptabilisation

Objectif: Implémenter AAA sur les routeurs Cisco en utilisant la base de données de routeur local du routeur et ACS ou un ISE.

## Chapitre 4: Implementation des technologies de parefeu

Objectif: Implémenter des technologies de pare-feu pour sécuriser la périphérie d'un réseau.

## Chapitre 5: Implementation de la prévention d'intrusion

Objectif: Implémenter des IPS pour atténuer des attaques réseaux

## Chapitre 6: Sécurisation du réseau local

Objectif: Sécuriser le périphérique finaux et atténuer les attaques de couche 2.

## Chapitre 7: Les systèmes cryptographiques

Objectif: Sécuriser des communications pour assurer l'intégrité, l'authenticité et la confidentialité.

## Chapitre 8: Implementation des réseaux privés virtuels

Objectif: Implémenter des VPN sécurisés.

## Chapitre 9: Implementation de Cisco Adaptive Security Appliance (ASA)

Objectif: implémenter le configuration d'un pare-feu ASA en utilisant le mode CLI

## Chapitre 10: Implementation avancée de Cisco ASA

Objectif: Implémenter la configuration d'un pare-feu ASA et VPNs en utilisant l'ASDM

## Chapitre 11: la gestion d'un réseau sécurisé

Objectif: Tester la sécurité du réseau et créer une politique de sécurité technique.

Si la plupart des gens choisissent le groupe INSIM, c'est parce qu'ils savent qu'ils y trouveront les meilleures conditions susceptibles de les préparer à bien gérer leur carrière