

Certification Cisco CCNP Security – Cisco Certified Network Professional

CATEGORIE : B

Vue d'ensemble

Domaine(s) d'activité professionnel dans lequel(s) est utilisé la certification :

Transverse : ■ **Tout secteur d'activité sauf artisanat**

Tout type d'entreprise ou association à partir de quelques postes informatisés et périphériques reliés en réseau, et entreprises du secteur informatique (conseil, vente) à partir d'une personne

Code(s) NAF : —

Code(s) NSF : **326**

Code(s) ROME : **M1810**, **M1806**, **M1804**, **M1802**, **M1801**

Formacode : —

Date de création de la certification : **24/08/2010**

Mots clés : **sécurité informatique**, **sécurité cisco**, **sécurité réseaux**, **CCNP sécurité**

Identification

Identifiant : **579**

Version du : **22/06/2015**

Références

Consensus, reconnaissance ou recommandation :

Formalisé :

- [Programme de certification requis pour les entités du réseau partenaires Cisco Channel Business Partner :](#)
- [Procédure qualité concernant le passage des examens Cisco](#)
- [Information Assurance Supplemental Resources, norme CNSS 4013](#)
- [Détails sur le programme de certification professionnel CISCO sur le site de l'éditeur :](#)

Non formalisé :

- [Etude des certifications informatiques les plus reconnues et les plus rémunératrices :](#)
- [Classement des titres de certification informatique les plus demandés :](#)

Norme(s) associée(s) :

—

Descriptif

Objectifs de l'habilitation/certification

La certification Cisco Certified Network Security Professional (CCNP Security) est aligné spécifiquement au métier de l'ingénieur de sécurité réseau responsable de la sécurité au niveau des routeurs, commutateurs, équipements, ainsi que des choix de mise en réseau, du déploiement, du dépannage des pare-feu, VPNs et solutions IDS / IPS.

Il pourra évoluer aisément vers un poste de responsable ou directeur de la sécurité des Systèmes d'Information, rôle crucial dans les entreprises qui mettent en œuvre une politique de protection des données et de la sécurité des systèmes d'information.

Lien avec les certifications professionnelles ou les CQP enregistrés au RNCP

- 4245
- 9857
- 12112
- 7440
- 14507

Descriptif général des compétences constituant la certification

Le candidat à la certification CCNP Security maîtrise les fonctionnalités avancées de sécurité présentes sur les équipements Cisco dédiés tels que Firewall, IPS, ou switches VPN, et est évalué sur les compétences suivantes :

Etre en mesure de développer une infrastructure de sécurité réseau
Identifier les menaces et les vulnérabilités du réseau
Mettre en œuvre les solutions pour se protéger des menaces
Installer, dépanner et contrôler les équipements pour garantir l'intégrité du réseau, la confidentialité des données et la disponibilité des appareils.

Modalités générales

Pour la préparation à la certification, est proposée aux candidats une formation pouvant aller jusqu'à 4 modules de 5 jours chacun, délivrée en classe avec un instructeur (en présentiel ou à distance), incluant des labs pratiques et des ressources complémentaires.

Liens avec le développement durable

Aucun

Public visé par la certification

- Salariés
- Demandeurs d'emploi

Valeur ajoutée pour la mobilité professionnelle et l'emploi

Pour l'individu

La certification Cisco CCNP Security est un véritable gage d'une expertise technique, elle atteste le rôle d'ingénieur réseau Sécurité et renforce la crédibilité professionnelle de son détenteur.

Grâce à ce titre de certification, son détenteur pourra prétendre à de nombreuses opportunités de carrière en tant que spécialiste Sécurité (RSSI).

L'organisme certificateur Cisco met en relation les professionnels qualifiés et nouvellement certifiés avec le réseau des partenaires de distribution Cisco qui recherche de nouveaux collaborateurs, à travers l'outil Partner Talent Cisco Network.

Pour l'entité utilisatrice

Les entités employant du personnel certifié Cisco CCNP Security maximisent leurs investissements matériels et surtout garantissent la protection des données de l'entreprise et sont mieux armées pour déjouer les menaces extérieures. Le thème de la sécurité étant l'une des problématiques majeures des directions informatiques, les spécialistes sont très recherchés.

Les professionnels certifiés CCNP Security sont également recherchés par les entités visant à entrer dans le programme Cisco Channel, avec une spécialisation en sécurité ou à maintenir leur accréditation.

L'organisme certificateur Cisco met en relation les professionnels qualifiés et nouvellement certifiés avec le réseau des partenaires de distribution Cisco qui recherche de nouveaux collaborateurs, à travers l'outil Partner Talent Cisco Network.

Evaluation / certification

Pré-requis

Indépendamment de l'âge ou du niveau scolaire initial, les candidats doivent posséder des connaissances en technologies réseaux Cisco, et notamment posséder le titre de certification CCNA Security pour valider leur titre de certification CCNP Security.

Compétences évaluées

Le candidat à la certification CCNP Security maîtrise un grand nombre de technologies et équipements de sécurité Cisco ; il est également évalué sur les compétences suivantes :

Etre en mesure de déployer Cisco Identity (ISE) et un accès sécurisé au réseau 802.1X mettre en œuvre et gérer la sécurité d'accès au réseau en utilisant la solution de produit de l'appareil Cisco ISE

Configurer un périmètre de sécurité utilisant des commutateurs Cisco, des routeurs Cisco, des pare-feux et Cisco Adaptive Security Appliance (ASA)

Mettre en œuvre et gérer la sécurité sur les firewalls Cisco ASA, les routeurs Cisco avec le pare-feu ensemble de fonctionnalités, et commutateurs Cisco

Protéger les données traversant une infrastructure publique ou partagée tels que l'Internet par la mise en œuvre et la maintenance de solutions VPN Cisco et le dépannage d'accès à distance et des solutions de site à site VPN

Déployer la gamme Cisco ASA Next-Generation Firewall (NGFW), ainsi que la sécurité web, la sécurité des e-mails

Niveaux délivrés le cas échéant (hors nomenclature des niveaux de formation de 1969)

-

La validité est Temporaire

Le titre Cisco CCNP Security est valable 3 ans, et doit être renouvelé avant l'échéance en réussissant un examen en vigueur de même niveau (CCNP), ou bien en acquérant un titre de niveau supérieur (CCIE)

Possibilité de certification partielle : oui

Étendue de la certification partielle :

La certification peut être obtenue en plusieurs étapes certificatives indépendantes

Quatre examens indépendants, qui peuvent être passés dans n'importe quel ordre : SENSS, SITCS, SISAS, SIMOS

Durée de validité des composantes acquises :

Certificateur(s)

- CISCO

Centre(s) de passage/certification

- De nombreux centres Pearson Vue France entière.

Chaque composant est valable 3 ans, tant qu'il n'existe pas de nouvelle version d'examen pour le programme équivalent.

Durée accordée pour valider les composantes manquantes :

Le candidat doit réussir les examens composant la certification CCNP

Security dans les 3 ans

Matérialisation officielle de la certification :

Un Certificat électronique est envoyé dans les 3 à 5 jours, puis un

certificat imprimé dans les 6 à 8 semaines.

Plus d'informations

Statistiques

La certification CCNP Security existe depuis de nombreuses années (autrefois connue sous le titre CCSP - Cisco Certified Security Professional)

Bien que Cisco ne publie pas le nombre des professionnels certifiés, sur environ 500 à 700 candidats qui passent l'examen de certification du niveau CCNP en France chaque année, on estime à 200 ceux qui choisissent d'entrée la spécialisation sécurité.

Autres sources d'information

<http://www.vue.com/cisco/>