Méthode pédagogique

Alternance de cours collectifs et de travaux pratiques individualisés sur équipements CISCO, encadrés par des instructeurs reconnus par le programme CISCO Networking Academy.

Intervenants

Formateurs certifiés CCNA/CCNP

Validation

Passage des tests en ligne spécifiques à chaque module CCNA.
Chaque chapitre est validé par un test final et par une étude de cas en laboratoire

Coût de la formation

Tarif «conventionné employeur» : 700 € par module / personne (repas compris)

Tarif «individuel payant» : 500 € par module / personne (repas compris)

Lieux de formation

IUT, Département Réseaux et Télécommunications
40 avenue de Soweto - Terre Sainte.
Saint-Pierre

Contact

IUT, Pôle Formation Continue et Alternance
secrétariat :
fc-iut@univ-reunion.fr
tel : 02 62 96 29 60
responsable pédagogique :
joel.grouffaud@univ-reunion.fr

iut.univ-reunion.fr
IUT de La Réunion Officiel

Mise à jour : 5 juillet 2017

Administration de réseaux

Certification académique CISCO Networking Academy - sécurité -

Objectifs de la formation

Cette formation est une introduction aux concepts fondamentaux de la sécurité et aux compétences nécessaires à l'installation, au dépannage et à la surveillance des périphériques réseau afin d'assurer l'intégrité, la confidentialité et la disponibilité des données et des équipements. CCNA Sécurité prépare les participants au monde du travail et à la certification Cisco CCNA Security reconnue dans le monde entier.

Public concerné

Cette formation s'adresse aux personnes désirant acquérir les principales notions relatives à la sécurité des réseaux, et qui souhaitent développer des compétences dans l'installation, la maintenance et la surveillance des technologies et équipements de sécurité Cisco.
Cette formation prépare à la certification professionnelle 210-260 INS (Implementing Cisco Network Security).

Pré-requis

Il est recommandé, sans que cela ne soit obligatoire, d'avoir suivi les modules 1 et 2 du CCNA routage et commutation, ou de posséder des connaissances équivalentes.

Programme (32 heures)

Chapitre 1 : Nouvelles menaces de sécurité des réseaux

Chapitre 2 : Sécuriser les périphériques réseau

Niveaux de privilège d'accès et rôles, Monitoring avec SNMP et serveur Syslog, Module de sécurisation automatique de l'IOS

Chapitre 3 : Authentication, Authorization, and Accounting (AAA)

Techniques AAA, Serveurs TACACS+ et RADIUS

Chapitre 4 : Mise en œuvre des technologies de pare-feu (firewall)

ACL avancés, Principes des firewalls, Politiques de zones

Chapitre 5 : Mise en œuvre de la prévention d'intrusion

Configuration des IPS, Mise à jour des bases de données IPS

Chapitre 6 : Sécurisation d'un réseau local

Contre mesure des attaques de couche 2 sur un commutateur (VLAN, STP, MAC, DHCP, etc.), Sécurité des ports d'un commutateur

Chapitre 7 : Systèmes cryptographiques

Cryptage, hachage, Signature numérique, intégrité, authentification, etc., Cryptographie à clé publique

Chapitre 8 : Mise en oeuvre d'un VPN

VPN IPSec site à site via la ligne de commande et avec le logiciel CCP

Chapitre 9 : Configuration du firewall Cisco ASA (Adaptive Security Appliance)

Principe et configuration d'un ASA

Chapitre 10 : Configuration avancée du firewall ASA

Mise en œuvre du VPN sur un ASA.

Chapitre 11 : Gestion d'un réseau sécurisé

Politique de sécurité, Outils et tests de la sécurité d'un réseau

Calendrier

jusqu'au 27 oct 2017	27, 28, 30 novembre et 1er décembre 2017
Inscriptions	Formation