CCNA Security

CCNA Security Certification répond aux besoins des professionnels de l'informatique qui sont responsables de la sécurité du réseau. Il confirme les compétences d'un technicien pour le placement, par exemple, les spécialistes de la sécurité réseau, administrateurs de la sécurité, les ingénieurs du support et de la sécurité réseau. Cette certification valide les compétences y compris l'installation, le dépannage et le contrôle des périphériques réseau afin de maintenir leur compétence intégrité, la confidentialité et la disponibilité des données et des dispositifs et se développe dans les technologies que Cisco utilise dans sa structure de sécurité.

Aux élèves de compléter la formation Cisco acquerront une introduction aux technologies de sécurité de base ainsi que la façon d'élaborer des politiques de sécurité et atténuer les risques. IT des organisations qui emploient CCNA Security, les titulaires de l'avoir du personnel qui peut se développer une infrastructure de sécurité, de reconnaître les menaces et les vulnérabilités des réseaux, et d'atténuer les menaces à la sécurité.

Ce cours est le besoin d'avoir la certification de l'AIIC / CNAP CCNA

La méthodologie de l'enseignement est une combinaison de quatre éléments:
• Salle de classe-laboratoire avec des professeurs hautement qualifiés certifiés dans la spécialité.
• Guide de certification de la qualité publié par Cisco Press.
• Les pratiques réelles.

Examen 640-553 IINS: Implementing Cisco IOS Network Security

Describe the security threats facing modern network infrastructures
Describe and list mitigation methods for common network attacks
Describe and list mitigation methods for Worm, Virus, and Trojan Horse attacks
Describe the Cisco Self Defending Network architecture

Secure Cisco routers
Secure Cisco routers using the SDM Security Audit feature
Use the One-Step Lockdown feature in SDM to secure a Cisco router
Secure administrative access to Cisco routers by setting strong encrypted passwords, exec timeout, login failure rate and using IOS login enhancements
Secure administrative access to Cisco routers by configuring multiple privilege levels
Secure administrative access to Cisco routers by configuring role based CLI
Secure the Cisco IOS image and configuration file

Implement AAA on Cisco routers using local router database and external ACS
Explain the functions and importance of AAA
Describe the features of TACACS+ and RADIUS AAA protocols
Configure AAA authentication
Configure AAA authorization
Configure AAA accounting

Mitigate threats to Cisco routers and networks using ACLs
Explain the functionality of standard, extended, and named IP ACLs used by routers to filter packets
Configure and verify IP ACLs to mitigate given threats (filter IP traffic destined for Telnet, SNMP, and DDoS attacks) in a network using CLI
Configure IP ACLs to prevent IP address spoofing using CLI
Discuss the caveats to be considered when building ACLs

Implement secure network management and reporting
Use CLI and SDM to configure SSH on Cisco routers to enable secured management access
Use CLI and SDM to configure Cisco routers to send Syslog messages to a Syslog server

Mitigate common Layer 2 attacks
Describe how to prevent layer 2 attacks by configuring basic Catalyst switch security features

Implement the Cisco IOS firewall feature set using SDM
Describe the operational strengths and weaknesses of the different firewall technologies
Explain stateful firewall operations and the function of the state table
Implement Zone Based Firewall using SDM

Implement the Cisco IOS IPS feature set using SDM
Define network based vs. host based intrusion detection and prevention
Explain IPS technologies, attack responses, and monitoring options
Enable and verify Cisco IOS IPS operations using SDM

Implement site-to-site VPNs on Cisco Routers using SDM
Explain the different methods used in cryptography
Explain IKE protocol functionality and phases
Describe the building blocks of IPSec and the security functions it provides
Configure and verify an IPSec site-to-site VPN with pre-shared key authentication using SDM