IINS - Implementing Cisco iOS Network Security

5 j (35 heures) Ref : IINS

Public

Ingénieurs réseaux, techniciens réseaux, administrateurs réseaux, professionnels réseaux souhaitant acquérir des compétences dans le domaine de l'intégration de la politique de sécurité dans un réseau déjà existant

Pré-requis

Avant de suivre cette formation, le participant doit posséder les
connaissances suivantes :
Connaissances et compétences équivalentes à la formation Cisco ICND1
Connaissances et compétences sur le système d'exploitation Windows

Moyens pédagogiques

Formation réalisée en présentiel ou à distance selon la formule retenue
Exposés, cas pratiques, synthèse, assistance post-formation pendant trois mois
Un poste par stagiaire, vidéoprojecteur, support de cours fourni à chaque stagiaire

Modalités de suivi et d'évaluation

Feuille de présence émargée par demi-journée par les stagiaires et le formateur
Exercices de mise en pratique ou quiz de connaissances tout au long de la formation permettant de mesurer la progression des stagiaires
Questionnaire d’évaluation de la satisfaction en fin de stage
Auto-évaluation des acquis de la formation par les stagiaires
Attestation de fin de formation

Objectifs

Contrer les menaces contre les systèmes IT
Déployer et intégrer les mesures sécuritaires
Protéger les éléments du réseau et de l’infrastructure
Développer les contrôles de menaces et les technologies de détection des dangers

Programme détaillé

L'ESSENTIEL DE LA SECURITE DES RESEAUX

Présentation des concepts de la sécurité des réseaux
Assimiler les stratégies de sécurité à l'aide d'une approche de continuité de services

Elaborer une stratégie de sécurité pour les réseaux Borderless

PROTEGER L'INFRASTRUCTURE DES RESEAUX

Présentation de la protection des réseaux Cisco

A l'aide de Cisco Configuration Professional, protéger l'infrastructure réseau

Mettre en place la sécurisation du plan de management de l'IOS Cisco

Paramétrer AAA sur l'IOS Cisco à l'aide de Cisco Secure ACS

Mettre en place la sécurisation du plan de données sur les switchs Catalyst Cisco

Mettre en place la sécurisation du plan de données dans les environnements IPv6

CONTROLER ET LIMITER LES MENACES

Organiser un plan de contrôle des menaces

Concevoir des listes de contrôle d'accès pour limiter les menaces

Assimiler les essentiels des pare-feux

Concevoir et intégrer les politiques de de pare-feux de l'IOS Cisco

Paramétrer les politiques de base des pare-feux sur les équipements Cisco ASA

Assimiler les essentiels de IPS

Configurer CISCO IOS IPS

METTRE EN PLACE LA CONNECTIVITE SECURISEE

Assimiler l'essentiel des technologies VPN

Présentation de l'infrastructure à clé publique PKI

Analyser l'essentiel d'IPSec

Configurer les VPNs site à site sur les routeurs Cisco IOS

Configurer les SSL VPNs à l'aide des équipements Cisco ASA