



# Implementing Cisco IOS Network Security

## Objectifs

Après avoir suivi le cours, les stagiaires seront capables de :

- Expliquer de façon pertinente une politique de sécurité pour contrecarrer les menaces sur le système d'information
- Configurer les routeurs de périphérie grâce aux fonctionnalités de sécurité intégrées au Cisco IOS
- Configurer les différents éléments des firewalls incluant les Access Control List (ACL) et le firewalling en zone
- Configurer un VPN IPsec site à site
- Activer et Configurer l'Intrusion Prevention System (IPS) intégré dans le Cisco IOS
- Paramétrer les équipements niveau 2 pour le contrôle d'accès et stopper les attaques orientées LAN

IINS

Version : 1.0  
5 jours

## A qui s'adresse ce cours ?

Ce cours s'adresse aux administrateurs, ingénieurs et techniciens réseaux ainsi qu'aux architectes réseaux ayant besoin de savoir comment définir et intégrer la politique de sécurité dans un réseau existant.

## Pré-requis

Il est recommandé de suivre le cours ICND1 avant de suivre ce cours et d'avoir des connaissances dans le système d'exploitation Microsoft Windows.

## Contenu du stage

### 1. Introduction aux principes de sécurité réseau

- 1.1. Les fondamentaux de la sécurité réseau
- 1.2. Etude des méthodologies d'attaque
- 1.3. Opérations de sécurité
- 1.4. Comprendre et développer une politique de sécurité pertinente
- 1.5. Construire le Cisco Self-Defending Network

### 2. Périmètre de sécurité

- 2.1. Sécuriser l'accès administratif aux routeurs Cisco
- 2.2. Introduction au Cisco Security Device Manager (SDM)
- 2.3. Configuration du AAA avec base locale sur un routeur
- 2.4. Configuration du AAA avec l'Access Control Server (ACS) sur un routeur
- 2.5. Implémentation du reporting et du management sécurisé
- 2.6. Blinder le routeur Cisco

### 3. Cisco IOS Firewall

- 3.1. Introduction aux technologies firewall
- 3.2. Création de filtres grâce aux Access Control Server (ACL)
- 3.3. Configurer le firewall en mode Zone-Based

### 4. VPN Site à Site

Pour plus d'informations : [info@learneo.com](mailto:info@learneo.com) ou 01 53 20 37 00



- 4.1. Introduction aux services cryptographiques
- 4.2. Explication du chiffrement symétrique
- 4.3. Explication des signatures digitales et des fonctions de hachage
- 4.4. Explication du chiffrement asymétrique et des PKI
- 4.5. Fondamentaux IPsec
- 4.6. Construire un tunnel IPsec Site à site en CLI
- 4.7. Construire un tunnel IPsec Site à site via le SDM

## 5. Cisco IPS

- 5.1. Introduction aux technologies IPS
- 5.2. Configuration de l'IPS via le SDM

## 6. LAN, SAN, Voix et sécurisation du poste utilisateur

- 6.1. Explication de la sécurité du poste utilisateur
- 6.2. Explication de la sécurité du SAN
- 6.3. Explication de la sécurité de la voix
- 6.4. Réduction des attaques niveau 2

## Déroulement du stage

	Jour 1	Jour 2	Jour 3	Jour 4	Jour 5
MATIN	Introduction Fondamentaux de la sécurité	Sécurisation de l'accès au routeur	Technologies Firewall	Service cryptographique	IPS
Déjeuner					
APRES-MIDI	Cisco SDN	AAA et reporting	ACL Zone-Based Firewall	Site à Site VPN	Sécurité SAN Sécurité Voix Attaques LAN

## Laboratoires pratiques

- Lab 1-1: Insertion de mot de passe avec la stéganographie
- Lab 1-2: Scan d'un poste client
- Lab 1-3: Scan d'un réseau
- Lab 2-1: Sécurisation de l'accès administratif d'un routeur
- Lab 2-2: Configuration du AAA via la base locale du routeur
- Lab 2-3: Configuration du AAA via le serveur ACS sur un routeur
- Lab 2-4: Implémentation du reporting et du management sécurisé
- Lab 2-5: Utilisation des outils SDM: One-Step Lockdown et Security Audit
- Lab 3-1: Configuration du filtrage via les ACLs
- Lab 3-2: Configuration du firewall en mode Zone-based
- Lab 4-1: Configuration d'un tunnel VPN Site à Site
- Lab 5-1: Configuration du Cisco IPS
- Lab 6-1: Fonctionnalités de sécurité sur les switches

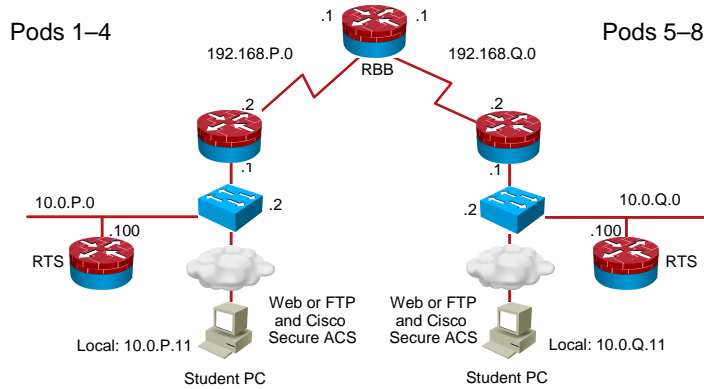
Pour plus d'informations : [info@learneo.com](mailto:info@learneo.com) ou 01 53 20 37 00

CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Networking Academy are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this Web site are the property of their respective owners.



## IINS Lab Topology



© 2008 Cisco Systems, Inc. All rights reserved.

IINS v1.0-1

## Visual Objective for Lab 1-1: Embedding a Secret Message Using Steganography

1. Create a secret message.
2. Embed it in a picture file.
3. Reveal the secret message.



© 2008 Cisco Systems, Inc. All rights reserved.

IINS v1.0-2

Pour plus d'informations : [info@learneo.com](mailto:info@learneo.com) ou 01 53 20 37 00

CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Networking Academy are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this Web site are the property of their respective owners.