Réseaux privés virtuels (VPN), mise en œuvre

Cours Pratique de 4 jours
Réf : VPI - Prix 2022 : 2 590€ HT

Cette formation vous apprend à concevoir, mettre en place et administrer un réseau privé virtuel VPN, dans le cadre de l'architecture IPSEC en environnement Linux, Cisco ou hétérogène. Les solutions sont analysées et comparées afin d'en connaître les avantages et incovénients.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Connaître les différentes caractéristiques et propriétés des principaux réseaux VPN

Maîtriser les apports d'ISAKMP sur le champ de la sécurité

Créer une politique de sécurité et de règles de filtrage

Configurer et administrer un VPN

MÉTHODES PÉDAGOGIQUES

Pédagogie active basée sur des échanges, des exemples, des exercices pratiques et une évaluation tout au long de la formation.

TRAVAUX PRATIQUES

Comporte des sessions magistrales qui présentent les concepts, mécanismes et informations nécessaires à une bonne maîtrise des VPN.

PARTICIPANTS

Ingénieurs systèmes, administrateurs réseaux, consultants, architectes et responsables de sécurité.

PRÉREQUIS

Bonnes connaissances en systèmes et réseaux.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

LE PROGRAMME

dernière mise à jour : 06/2021

1) Introduction

- Faiblesses propres aux réseaux TCP/IP.
- Impératifs du réseau d'entreprise.
- Solution "Réseau Privé Virtuel".

2) Solutions d'interconnexion IP

- TCP/IP : rappels. Principaux protocoles de la pile.
- Technologies RTC, RNIS, Internet et xDSL.
- Les bases du sans-fil. La technologie MPLS.

3) Cryptographie

- Les besoins numériques. Document, échange : authentification sûre.
- Chiffrements symétrique, asymétrique et autorités de certification.
- Authentification et signature électronique
- La non-répudiation.
- Cryptographie et réseaux privés virtuels.

4) Tunnels, les protocoles

- Point-to-Point Tunneling Protocol (PPTP), L2F, L2TP.
- IPSec, le standard IETF. Authentification, confidentialité, intégrité, anti-rejeu.
- Modes tunnel et transport. SA (Security Association), SPD (Security Policy Database).
- Protocoles ESP et AH.

Travaux pratiques : Réalisation d'un tunnel SSH over PPP. Mise en oeuvre de deux passerelles VPN over SSH.

5) ISAKMP et IKE

- En-tête ISAKMP. Les phases de négociation.
- Le Pre-Shared Key, les certificats. La phase 1 et la phase 2. L'agressive mode. Le mode config, Xauth.

Travaux pratiques : Exemples et analyse des échanges.

6) Sécurité de l'infrastructure réseau

- Rôle du firewall. Authentification des utilisateurs. Faiblesses de la solution login/mot de passe.
- Solution SecurID. Protocole Kerberos. Certificats.
- RADIUS et LDAP. Sécurité du poste client, le maillon faible.
- OS, firewall personnel, antivirus, sensibilisation des utilisateurs.
- WiFi et réseaux privés virtuels.

Travaux pratiques : Utilisation de protocole IPSec en mode transport dans un réseau sous Windows. Création d'une politique de sécurité et de règles de filtrage.

7) L'offre

- VPN, firewall, Internet Appliance et Open Source.
- Les clients VPN. L'outil Open VPN.
- Les plates-formes VPN : routeurs, firewalls, VPN firewall, concentrateurs VPN, le VPN Appliance.

Travaux pratiques : Mise en place d'OpenVPN. Exemples de configuration en site-to-site et client-to-site.

LES DATES

PARIS LA DÉFENSE
2022 : 13 sept., 13 déc.

CLASSE A DISTANCE
2022 : 13 sept., 13 déc.