

VPN sécurisé pour le télétravail et interconnexion de sites

3 jours (21 heures)

Perfectionnement

Présentiel ou classe à distance

à partir de

2 085 € HT par personne (TVA en vigueur) **Repas inclus en présentiel**

Contenu mis à jour le 25/09/2026. Document téléchargé le 07/10/2026.

Objectifs

A l'issue de cette formation, vous serez capable de :

- Mettre en oeuvre un réseau privé virtuel sur les réseaux filaires comme sur les réseaux sans-fil
- Identifier les menaces contre vos communications
- Déterminer les coûts, la sécurité et le choix des technologies
- Appliquer les techniques de chiffrement des messages
- Décrire les offres des opérateurs
- Mettre en place une politique de détection, correction des failles et vulnérabilités dans les réseaux.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Professionnels de la sécurité, administrateurs, ingénieurs réseau, responsables de sites Web, responsables de communication et responsables informatiques.

Prérequis

Avoir une bonne connaissance des protocoles TCP/IP, une pratique de l'Internet et des applications standards.

Programme

1 Pendant votre formation

VPN sécurisé pour le télétravail et interconnexion de sites

Jour 1

Présentation : assurer des communications sûres dans un environnement hostile

- Organisations étendues et mobilité
- Menaces sur les communications
- Assurer la sécurité des communications

Rappels sur l'encapsulation et la Qualité de Service (QoS)

- TCP/IP et la modélisation OSI
- Serial Line Interface Protocol (SLIP), Point-to-Point Protocol (PPP), Point-to-Point Tunneling Protocol (PPTP)
- Level 2 Forwarding (L2F)
- Layer 2 Tunneling Protocol (L2TP)
- Multiprotocol Label Switching (MPLS)
- QoS, intserv et diffserv

Réseaux Virtuels Privés (VPN)

- Qu'est-ce qu'un VPN ?
- Utilisations et environnement
- "Monter" un VPN

Exemples de travaux pratiques (à titre indicatif)

- Généralités sur les réseaux privés virtuels (VPN)
 - Comprendre les concepts fondamentaux des VPN
 - Explorer les différents types de VPN
 - Configurer et déployer un VPN pour sécuriser les communications
 - Tester et évaluer les performances et la sécurité du VPN

Jour 2

Sécurité des VPN

- Présentation des différentes technologies et protocoles
- Notions de sécurisation du transport des données

Chiffrement

- Transformation des messages : chiffrement et déchiffrement
- Principaux types de chiffrement
- Signatures numériques

- Certificats numériques
- Mise en place des protections
- Validation, révocation, automatique et manuelle des clés

Gestion de clés publiques (PKI)

- Objectifs de la PKI
- Caractéristiques et éléments de la PKI
- Exemples de PKI

Déploiement de communications sécurisées

- Identification des risques, politique à mettre en place et architecture
- Installation des services de protection
- Sécurité des communications et disponibilité
- Identifier les applications à protéger et choix de solutions

Protocole IPsec

- Qu'est-ce que IPsec ?
- Association de sécurité (SA)
- Base de données de sécurité (SADB)
- Base de données des procédures (SPD)
- Mode opératoire et services de sécurité d'IPsec
- Phases et échanges de clés Internet (IKE)
- IKEV2
- Risques et limites d'IPsec
- Principaux matériels / logiciels permettant de créer des VPN IPsec

Sécurité des couches applicatives : SSL, SSH et TLS

- Qu'est-ce que SSL / TLS ?
- Mode opératoire et services de sécurité de SSL / TLS
- Risques et limites de SSL / SSH
- Principaux matériels / logiciels permettant de créer des VPN SSL / TLS / SSH

Exemples de travaux pratiques (à titre indicatif)

- *Généralités sur les réseaux privés virtuels (VPN) avec IPsec et SSL/TLS*
 - Comprendre les principes de base des VPN avec IPsec et SSL/TLS
 - Configurer et déployer un VPN IPsec (règles routage et firewall)
 - Configurer et déployer un VPN SSL/TLS
 - Comparer les avantages et les inconvénients des deux implémentations VPN

Jour 3

Modèles propriétaires : LEAP, WPA, VNC...

- Communications sans fils et sécurité
- Solutions propriétaires
- L'heure du choix !

Maintien en conditions opérationnelles des communications sécurisées

- Principes pour maintenir et gérer des communications sécurisées
- Analyse et correction des fautes
- Gestion des performances
- Gestion des clés
- Les évolutions
- Sécurité et IPv6

Exemples de travaux pratiques (à titre indicatif)

- Effectuer un diagnostic d'une perte de liaison VPN
- Analyser le débit et le split tunneling

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* nous consulter pour la faisabilité en distanciel

** ratio variable selon le cours suivi

Accessibilité aux personnes en situation de handicap

Détails de la session

Du 5 janvier 2027 au 7 janvier 2027 (3 jours / 21 heures)

À distance

Du 5 janvier 2027 au 7 janvier 2027 À distance

- 5 janvier 2027 9h00 - 16h00
- 6 janvier 2027 9h00 - 16h00
- 7 janvier 2027 9h00 - 16h00