

## VPN - Préserver ses informations sur internet

### Organisation

---

Mode d'organisation : Présentiel ou distanciel

Durée : 3 jour(s) · 21 heures

### Contenu pédagogique

---



#### Type

Action de formation



#### Public visé

Professionnels de la sécurité, administrateurs, ingénieurs réseau, techniciens informatiques  
Cette formation est accessible aux publics en situation de handicap et aux personnes à mobilité réduite. Des aménagements peuvent être prévus en fonction des profils. Nous contacter pour plus d'information.



#### Prérequis

Bonne compréhension des protocoles TCP/IP, pratique de l'Internet et des applications standards



#### Objectifs pédagogiques

Connaitre les menaces de vos communications internes, inter sites, nomades

Appréhender les opportunités technologiques

Bonnes pratiques pour leur mise en service, leur suivi et leur contrôle



#### Description

VPN : Assurer des communications sûres dans un environnement hostile

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

Réseaux Virtuels Privés

- Qu'est-ce qu'un VPN ?
- Quelles utilisations ?
- Comment construire ou acquérir un VPN ?

Première approche de la cryptographie

- Transformation des messages – chiffrement et déchiffrement
- Deux types de chiffrements
- Signatures numériques
- Certificats numériques
- Implantation des protections
- Vieillessement et révocation automatique et manuelle des clés



### Gestion de clés publiques (PKI)

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

### Première approche de l'encapsulation et de l'étiquetage

- TCP/IP et le modèle OSI
- Serial Line Interface Protocol (SLIP), « Point to point protocole » (PPP), « Point to point Tunneling Protocol » (PPTP)
- Level 2 Forwarding (L2F), Layer 2 Tunneling Protocol (L2TP)
- Multiprotocol Label Switching (MPLS)
- Protocole de réservation de ressource (RSVP), services différenciés (DiffServ), et services intégrés IETF (IntServ)

### Sécurité du protocole IP (Ipsec)

- Qu'est-ce que l'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 échange de clés Internet (IKE)
- 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

### Modèles propriétaires : LEAP/WPA/VNC/

- La sécurité nécessaire des communications sans fils
- Des solutions cryptographiques propriétaires controversées
- Quelle harmonisation ?

### Architecture de communications sécurisées

- Applications à servir, répartition des risques, politique, et architecture
- Lieu d'installation des services de protection
- Sécurité des communications et disponibilité
- Approche de choix de solutions

### Gestion et maintenance des communications sécurisées

- Principes pour maintenir et gérer des communications sécurisées
- Recherche et correction des fautes
- Performance
- Gestion des clés
- Directions futures
- Services de sécurité dans IPV6



## Modalités pédagogiques

Réflexion de groupe et apports théoriques du formateur – Travail d'échange avec les participants sous forme de discussion – Utilisation de cas concrets issus de l'expérience

professionnelle – Exercices pratiques (études de cas, jeux de rôle, questionnaires, quiz, mises en situation, ...) sont proposés pour vérifier le niveau de compréhension et d'intégration du contenu pédagogique – Remise d'un support de cours complet pour référence ultérieure



## Moyens et supports pédagogiques

Accueil des apprenants dans une salle dédiée à la formation. Chaque participant disposera d'un ordinateur (si besoin), d'un support de cours, d'un bloc-notes et d'un stylo. La formation se déroulera avec l'appui d'un vidéoprojecteur et d'un tableau blanc.



## Modalités d'évaluation

### Avant la formation :

Nous mettons en place une évaluation de chaque participant via un questionnaire d'évaluation des besoins et de niveau.

Un audit complémentaire peut-être proposé pour parfaire cette évaluation

### Pendant la formation :

Des exercices pratiques (études de cas, jeux de rôle, questionnaires, quiz, mises en situation, ...) sont proposés pour vérifier le niveau de compréhension et d'intégration du contenu pédagogique.

### À la fin de la formation :

Le participant auto-évalue son niveau d'atteinte des objectifs de la formation qu'il vient de suivre.

Le formateur remplit une synthèse dans laquelle il indique le niveau d'acquisition pour chaque apprenant : « connaissances maîtrisées, en cours d'acquisition ou non acquises ». Il évalue ce niveau en se basant sur les exercices et tests réalisés tout au long de la formation.

Le participant remplit également un questionnaire de satisfaction dans lequel il évalue la qualité de la session.

À la demande du stagiaire, le niveau peut aussi être évalué par le passage d'une certification TOSA pour les outils bureautiques, CLOE pour les langues.



## Modalités de suivi

Emargement réalisé par 1/2 journée – Certificat de réalisation remis à l'employeur à l'issue de la formation – Assistance par téléphone et messagerie – Support de cours remis à chaque participant à l'issue de sa formation – Suivi de la progression 2 mois après la formation