



# TCP/IP - Mise en œuvre d'un réseau sécurisé

Mise à jour févr. 2025

**Durée** 4 jours (28 heures )

« Délai d'accès maximum 1 mois »

## OBJECTIFS PROFESSIONNELS

- Concevoir et mettre en oeuvre des réseaux TCP/IP.
- Principes et techniques d'interconnexion et d'administration. Mise en oeuvre des principales applications de TCP/IP

## PARTICIPANTS

- professionnels de la sécurité, les administrateurs, les ingénieurs réseau, technicien informatique

## PRE-REQUIS

- Avoir des notions d'administration système.

## MOYENS PEDAGOGIQUES

- Réflexion de groupe et apports théoriques du formateur
- Travail d'échange avec les participants sous forme de sous forme de réunion-discussion
- Utilisation de cas concrets issus de l'expérience professionnelle
- Validation des acquis par des questionnaires, des tests d'évaluation, des mises en situation et des jeux pédagogiques.
- Remise d'un support de cours.

## MODALITES D'EVALUATION

- Feuille de présence signée en demi-journée,
- Evaluation des acquis tout au long de la formation,
- Questionnaire de satisfaction,
- Positionnement préalable oral ou écrit,
- Evaluation formative tout au long de la formation,
- Evaluation sommative faite par le formateur ou à l'aide des certifications disponibles,
- Sanction finale : Certificat de réalisation, certification éligible au RS selon l'obtention du résultat par le stagiaire

## MOYENS TECHNIQUES EN PRESENTIEL

- Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs, d'un vidéo projecteur d'un tableau blanc et de paperboard. Nous préconisons 8 personnes maximum par action de formation en présentiel

## MOYENS TECHNIQUES DES CLASSES EN CAS DE FORMATION DISTANCIELLE

- A l'aide d'un logiciel comme Teams, Zoom etc... un micro et éventuellement une caméra pour l'apprenant,
- suivez une formation uniquement synchrone en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur.
- Les formations en distanciel sont organisées en Inter-Entreprise comme en Intra-Entreprise.
- L'accès à l'environnement d'apprentissage (support de cours, labs) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré. Nous préconisons 4 personnes maximum par action de formation en classe à distance

## ORGANISATION

- Les cours ont lieu de 9h à 12h30 et de 14h à 17h30.

## PROFIL FORMATEUR

- Nos formateurs sont des experts dans leurs domaines d'intervention
- Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité.

## A L'ATTENTION DES PERSONNES EN SITUATION DE HANDICAP

- Les personnes atteintes de handicap souhaitant suivre cette formation sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités de suivre la formation.

## Programme de formation

### VPN: Assurer des communications sûres dans un environnement hostile (02h00)

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

### Réseaux Virtuels Privés (02h00)

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

### Première approche de la cryptographie (03h45)

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

### Gestion de clés publiques (PKI) (02h00)

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

### Première approche de l'encapsulation et de l'étiquetage (03h15)

- 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) (03h45)

- 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 (02h30)

- 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/... (02h00)

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

### Architecture de communications sécurisées (02h30)

- 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 (03h45)

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