



FORMATION EXPERTISE : ANALYSE DE TRACES ET TROUBLE SHOOTING VOIP

OBJECTIFS

Ce cours apporte au stagiaire, les bases théoriques et la mise en pratiques réelles pour une maîtrise de la politique de qualité et de sécurité VoIP / ToIP.

A l'issue de la formation, les stagiaires seront capables de :

- appréhender les menaces et les attaques internes et externes du monde IP, les vulnérabilités
- décrire les critères de la qualité de service vocale, QoS et sécurité ToIP
- analyser et détecter pour résoudre les problèmes de codage de la voix, les solutions de cryptage
- analyser et détecter pour résoudre les problèmes de signalisation
- détecter pour résoudre les problèmes d'interconnexion entre opérateurs SIP, SIP-I, SIP-T / SS7
- comprendre les spécificités des architectures sécurisées et les impératifs de QoS
- recherche des causes de dysfonctionnement, utilisation de softphone

MÉTHODE

Formation essentiellement pratique. Tout au long de la formation, du temps sera consacré aux exercices et aux questions permettant d'intégrer les notions de base et de les manipuler en groupe.

L'atteinte des objectifs est contrôlée au fur et à mesure du stage.

PERSONNES CONCERNÉES, PRÉREQUIS

Ingénieurs, techniciens, administrateurs systèmes et réseaux ayant des connaissances en informatique, TCP/IP et VoIP et devant intervenir dans le déploiement de solutions VoIP/ToIP pour des opérateurs télécoms et de grandes entreprises.

DURÉE

Cette formation de trois jours est dispensée en langue française en intra entreprise pour 6 participants maximum.

Analyse des problématiques ToIP

- rappel sur les protocoles,
 - SIP
 - les messages 6xx
- travaux Pratique avec softphone et Etherreal/Wireshark
- analyse de traces
- fax en G711 In band et en T38, atouts et limite, causes des dysfonctionnements, solutions
- étude de traces Wire Shark d'appels qui posent problème
 - les stagiaires sont invités à apporter leurs traces, afin qu'elles soient étudiées pendant la formation, dans la mesure du temps disponible
- travaux Pratiques avec d'outils d'analyse et de supervision (par exemple ANRITSU, K18, ...), dans les situations d'interconnexion SS7 - SIP

Analyse des problématiques d'identification, Trouble Shooting

- identification/ Authentification des téléphones
- autorisation du proxy
- les messages 4xx
- travaux Pratique avec softphone et Etherreal/Wireshark

Analyse des problématiques de sécurité, Trouble Shooting

- techniques de translation d'adresses, limites, solutions
- Le filtrage des ports sur le firewall

Nous proposons d'utiliser les outils de l'opérateur pour superviser et analyser son trafic. Merci de nous préciser le nom de l'outil, et de vérifier l'accès de l'outil à partir de la salle de cours.