

# Résumé de la formation (2011-12-05)

## UTM Expert Plus v9 (NT-FWXP+-V9)

NETASQ N° d'agrément : 31.59.05307.59

### 1. Introduction

L'objectif de cette formation est de fournir des outils et méthodes pour rassembler les informations nécessaires, à l'étude et à la correction des problèmes en utilisant le CLI. Cette formation est à destination des sociétés souhaitant devenir NSCS ou NCTC (pour les apprenants ayant pour objectif de devenir un ingénieur support ou formateur expert sur nos produits UTM)

### 2. Lieu, durée et enregistrement

Cette formation est uniquement dispensée par les formateurs ou membres des équipes support de NETASQ.

NETASQ peut vous proposer une formation dans ses locaux de Villeneuve d'Ascq (France), ou de Boulogne Billancourt (France). Nos formateurs peuvent également se déplacer à l'étranger pour dispenser la formation.

La durée de la formation Expert Plus est de 3 jours. La formation débute à 9h30 le premier jour et à 9h00 les autres jours. Toute demande d'inscription doit être faite auprès du service formation NETASQ ([formation@netasq.com](mailto:formation@netasq.com)). Le nombre de participant est limité à 4 par session. Le matériel pédagogique est fourni à chaque participant.

### 3. Prérequis et matériel

Connaissances approfondies en TCP/IP et shell UNIX. Les apprenants doivent être certifiés CNE V9 et doivent venir avec un ordinateur portable sous Windows (ou tout autre système d'exploitation avec un logiciel de virtualisation et un Windows virtuel) afin de faire les exercices proposés. VirtualBox 3.1.x ou supérieur (<http://www.virtualbox.org/>) ou VMPlayer 3.0.x.

### 4. Description détaillée

#### 4.1 Jour 1

- Introduction
- Système d'exploitation et commandes UNIX liées
  - o Méthodes d'accès au shell et paramètres
  - o SSH : fonctionnalités
  - o Système de fichier et commandes associées
  - o Répertoires et commandes associées

- Environnement système et utilisateur
- Fichiers et commandes associées
- Logs
  - Logs locaux : localisation, catégories, indexation, nomenclature et syntaxe
  - Commandes associées
  - Fichiers de configuration
  - Paramètres d'export vers un syslog externe
  - logd : le démon logs ; verbose et synoptique
  - logctl : interagir avec le démon logs
- Fichiers de configuration et de sauvegarde
  - Localisation du répertoire et syntaxe générale
  - Commandes associées : setconf, debackup, enbackup, nsrpc, tar, defaultconfig
- Réseau et routage
  - Fichier de configuration réseau : exemple de paramétrage d'interfaces (avancé, bridged, protégé)
  - Bridge : comportement, paramétrages particuliers
  - Commandes associées au réseau
  - Routage : rappels (but et utilisation, priorités)
  - Paramètres et fichier de configuration de routage
  - Paramétrage de Gatemon
  - Commandes liées au routage
  - Interaction avec la table des adresses protégées
  - Gatemon verbose
- Capture et analyse de trafic avec tcpdump
  - Introduction et conseils
  - Syntaxe Générale
  - Filtres usuels
  - Exemples commentés
  - Conseil pour faire de bonnes captures
  - Analyse des résultats de tcpdump (flux TCP, UDP/icmp)

#### 4.2 Jour 2

- Démons et Processus
  - Liste et rôle
  - Superviseur présent
  - Commandes associées
- Objets
  - Fichiers de configuration et fichiers liés à UNIX
  - Commandes associées
- ASQ : analyses

- Analyse pas à pas des couches réseau
- Commande associée : sfctl
- Paramètres globaux
- Localisation et structure des profiles
- Note concernant les paramètres d'analyse de protocole
- ASQ asynchrone : cas, paquet "tag"
- ASQ verbose mode
- ASQ : politique de sécurité
  - Fichiers de configuration et syntaxe
  - Filtre : commandes associées
  - Filtre : exemple de règles chargées (action, niveau d'inspection, plugin, PBR, QoS, interfaces, proxy)
  - Filtre : translation d'objets groupes et de listes (tables), et opérateurs
  - NAT : rappels (NAT Dynamique, NAT Statique par port, NAT statique/Bimap, Non NAT)
  - NAT : commandes associées
  - NAT : exemples de NAT charge et mécanismes ARP associés
- ASQ : Stateful et tables d'états
  - Table d'adresses protégées
  - Table des hôtes
  - Table des connexions : exemples d'états de connexion (NAT, vconn, FTP plugin, async, lite...)
- Concepts et mécanismes FTP
  - Mécanismes des modes passif et actif
  - Règles de filtrages essentielles et non utilisées

### 4.3 Jour 3

- Eventd : démon de planification des événements
  - Utilisation et syntaxe
  - Exemples
- VPN IPsec
  - Mise en œuvre d'un IPsec NETASQ/IKE
  - Synoptique
  - Négociations IKE et clés dérivées
  - NAT-T, DPD, Keepalive, SharedSA, Politique None, SPD Cache
  - Commandes associées
  - Analyse d'un IPsec-SA
  - Logs et dépannage
  - Mode Verbose

## 5. Certification

Dans les deux mois suivant la formation, chaque participant peut passer un examen de certification Expert Plus. Cet examen dure 2h00 et permet de valider la certification CNEP.

Cet examen se compose de deux parties :

- Théorique, comportant des QCM et des questions ouvertes sur les généralités réseau, TCP/IP et fonctionnalités, paramétrages et des méthodes de dépannage des UTM NETASQ.
- Pratique, où vous devrez répondre à des rapports d'incidents venant de clients ; expliquer vos idées et méthodes et décrire en détail les actions que vous demanderiez à votre client en cas de demande d'information complémentaire de votre part.