

Fiche de synthèse formation

Administrateur UTM v9 (NT-FWADM-V9)

NETASQ organisme de formation agréé N° 31.59.05307.59

1. Introduction

Cette formation a pour but de présenter la gamme et les fonctionnalités de base du produit de prévention d'intrusions / UTM.

2. Lieu, durée et inscriptions

NETASQ se repose majoritairement sur son réseau de distribution et ses partenaires de formation afin de dispenser les formations.

La liste des centres de formation agréés NETASQ (NCTC) ainsi que le calendrier des sessions sont disponibles à l'adresse suivante :



<http://www.netasq.com/fr/produits-services/formations.php>

NETASQ vous propose des formations au sein de son siège social situé à Villeneuve d'Ascq (59), mais également dans ses locaux de Boulogne Billancourt (92). Nos formateurs peuvent également se déplacer à l'étranger pour assurer les formations.

La formation Administrateur se déroule sur trois jours insécables. Les stagiaires sont convoqués à 9h30 le premier jour de la formation. Toutes les demandes d'inscription doivent être envoyées à votre centre de formation certifié NETASQ (NCTC), ou au service formation NETASQ (formation@netasq.com). Les effectifs maximum sont de 8 personnes par session. Un support de cours est fourni à chaque stagiaire.

3. Pré-requis et matériel

Bonnes connaissances TCP/IP. Avoir suivi une formation IP préalable est un plus. Les stagiaires devront se munir d'un PC type portable avec un système d'exploitation WINDOWS afin de réaliser les exercices proposés au cours de la formation et également du logiciel VirtualBox en version 3.1.x ou plus (<http://www.virtualbox.org/>).

4. Description détaillée

4.1 Jour 1

- Présentation de la société et des produits (U, NG et V).
- Présentation des fonctions standards et optionnelles

- Les fonctions standards
- Les options logicielles et matérielles
- Présentation des packs de maintenance
- Prise en main du boîtier
 - Injection de la licence
 - Mise à jour de la version
 - Connexion sur le portail WEB et présentation du tableau de bord
 - Configuration système et droits d'administration
- Configuration réseau
 - Présentation des différents modes de configuration et des types d'interfaces
 - Notions de routage
 - Présentation des fonctionnalités serveur et relais DHCP
- Configuration de l'UTM et présentation des objets
 - Création d'objets
 - Présentation des objets dynamiques et particuliers
- Présentation du module de prévention d'intrusions
 - Profils et méthode d'analyse (basique)
 - Présentation du module de détection de vulnérabilités SEISMO (basique)
- Filtrage et matrice de flux
 - Généralités sur le filtrage et notion de stateful
 - Intérêt et présentation des méthodes d'inspection

4.2 Jour 2

- Configuration de la translation d'adresses (NAT)
 - Généralités et ordonnancement des règles
 - Mise en situation par le biais de scénarii explicatifs
- Protection applicative
 - Mise en place de différentes analyses applicatives
 - Mise en place d'analyses antivirale et antispam
- Authentification et Utilisateurs
 - Généralités et présentation des types de bases LDAP disponibles
 - Répartition des droits d'administration

4.3 Jour 3

- Les réseaux privés virtuels (VPN)
 - Présentation des différents types
 - Mise en situation par le biais de scénarii
- Gestion des logs et des alarmes

5. Certification

Au terme de ces trois jours de formation, un examen d'une durée de 1h30 aura lieu permettant ainsi de valider les connaissances et compétences acquises durant tout le cursus.

L'examen se divisera en deux parties:

- une partie théorique, constituée d'un QCM de 50 questions,
- et d'une partie pratique, constituée d'un scénario à réaliser (configuration réseau, routage, filtrage, NAT, création d'objets, ...).