kapedia
FORMATIONS INFORMATIQUES
systèmes | virtualisation | réseaux | messagerie | sécurité | développement | web | gestion de projets | sharepoint | SGBD | infographie | bureautique
www.kapedia.fr

F5 LTM ET ASM

Code **SECU31**	**Objectifs** Après avoir suivi la formation, les stagiaires seront en capacite *:* • D'administrer F5 Big IP • De configurer F5 LTM • De configurer iRule • De configurer F5 Advanced Web Application Firewall (known as ASM)
	Public Administrateurs F5 Big IP LTM, et F5 Advanced Web Application Firewall (known as ASM)
Durée **5 jours**	**Prérequis** Connaissance OS Windows/linux – Connaissance TCP / IP
	Méthodes pédagogiques Alternance d'apports théoriques et d'exercices pratiques.

Contenus des thèmes abordés

- Sauvegarder le système Big-IP
- Configurer des virtuals serveurs, pools, monitors, profiles et des persistence objects
- Tester et vérifier le fonctionnement du système avec les local traffic statistics
- Configurer des groupes de priorités et activer des pools de Load Balancing dynamiques
- Configurer des limites de connexions et définir un seuil de volume de traffic pour un membre du pool
- Définir les affinity persistence et leur usage
- Configurer les health monitors, voir les différents usages
- Configurer différents types de services virtuels et les différentes manières de gérer le trafic.
- Configurer les différents types de SNAT
- Configurer VLAN tagging et trunking
- Configuring les alertes SNMP
- Utiliser des iRules pour personnaliser les applications
- Configurer le Big-IP pour contrer des attaques de base.
- Configurer F5 Advanced Web Application Firewall (ASM)
- Définir le web application firewall
- Décrire comment le F5 Advanced Web Application Firewall protège une application web en sécurisant les types de fichiers, URLs et paramètres
- Deployer le F5 Advanced Web Application Firewall en utilisant des templates

- Définir l'apprentissage, les alarmes et les paramètres de blocage
- Définir les signatures d'attaques et expliquer l'importance du stagging
- Analyser les différences entre une stratégie positive et une négative et voir les avantages respectifs.
- Configurer le processing de la sécurité au niveau de l'application web
- Deployer F5 Advanced Web Application Firewall en utilisant l'Automatic Policy Builder
- Ajuster une stratégie manuellement ou en autorisant l'automatic policy building
- Configurer l'obligation de login
- Configurer la protection contre les brutes force attaques