# F5 Configuration BIG-IP Advanced Firewall Manager (AFM)

**Durée: 2 Jours** **Réf de cours: AFM** **Méthodes d'apprentissage: Intra-entreprise & sur-mesure**

## Résumé:

Apprenez à déployer et à utiliser BIG-IP Advanced Firewall Manager pour protéger un centre de données contre les menaces entrantes qui pénètrent dans le réseau au niveau des couches 3 et 4 sur des protocoles courants tels que HTTP, SIP, SSH, SSL et autres.
Grâce à une combinaison de cours magistraux et de travaux pratiques en laboratoire, vous acquerrez de l'expérience dans la mise en œuvre d'une protection complète contre les attaques provenant d'adresses IP qui changent rapidement, en appliquant les dernières informations sur les menaces et en anticipant, détectant et répondant aux attaques avant qu'elles n'atteignent les cibles du centre de données.
Pratiquez l'utilisation de l'atténuation DDoS matérielle qui s'adapte pour empêcher les attaques ciblées de gros volumes sur le réseau, tout en permettant au trafic légitime de circuler sans compromettre les performances ou dégrader l'expérience de l'utilisateur. Observez l'activité réseau malveillante en temps réel en vous mettant dans la peau d'un attaquant. F5 reconnaît l'importance de la visibilité, de l'analyse et des rapports concernant l'évolution des attaques, l'atténuation des attaques et la santé générale du pare-feu.
Beaucoup de temps est consacré à l'analyse des rapports. Apprenez à récupérer des informations claires, concises et exploitables mettant en évidence les attaques et les tendances grâce à des fonctionnalités détaillées d'exploration et de visualisation des pages.
Mis à jour 13/01/2025

Formation intra-entreprise

Cette formation est délivrable en session intra-entreprise, dans vos locaux ou dans les nôtres. Son contenu peut être adapté sur-mesure pour répondre aux besoins de vos collaborateurs. Contactez votre conseiller formation Global Knowledge ou adressez votre demande à info@globalknowledge.fr.

## Public visé:

Ce cours est destiné aux administrateurs système et réseau responsables de la configuration et de l'administration continue d'un système BIG-IP Advanced Firewall Manager (AFM).

## Objectifs pédagogiques:

- A l'issue de cette formation, les participants seront en mesure de :
- Configurer et gérer un système AFM
- Configurer le pare-feu réseau AFM dans un modèle de sécurité positif ou négatif
- Configurer le pare-feu réseau pour autoriser ou refuser le trafic réseau à l'aide de règles basées sur le protocole, la source, la destination, la géographie et d'autres types de prédicats.
- Pré-construire des règles de pare-feu à l'aide de listes et de composants de planification
- Appliquer les règles de pare-feu immédiatement ou les tester à l'aide d'une méthode de simulation de politique (policy staging)
- Utiliser les fonctions Packet Tester et Flow Inspector pour vérifier les connexions réseau par rapport à vos configurations de sécurité pour le pare-feu réseau, l'intelligence IP et les fonctions DoS.
- Configurer diverses fonctions d'intelligence IP pour identifier, enregistrer, autoriser ou refuser l'accès par adresse IP
- Configurer la fonction de détection et d'atténuation des dénis de service pour protéger l'appareil BIG-IP et toutes les applications
- Configurer et utiliser les logs locaux et distants de l'AFM
- Configurer et surveiller l'état d'AFM à l'aide de diverses fonctions de reporting.
- Exporter les rapports du système AFM vers votre système de surveillance externe directement ou par courrier programmé
- Permettre au trafic sélectionné de contourner les contrôles DoS à l'aide des listes blanches.
- Isoler les clients potentiellement mauvais des bons clients à l'aide de la fonction Sweep Flood (balayage des fluxIsoler et réacheminer le trafic réseau potentiellement mauvais en vue d'une inspection plus poussée à l'aide de la fonctionnalité IP Intelligence Shun
- Restreindre et signaler certains types de requêtes DNS à l'aide du pare-feu DNS
- Configurer, atténuer et signaler les attaques DoS basées sur le DNS à l'aide de la fonction DNS DoS
- Configurer, atténuer et signaler les attaques DoS basées sur le protocole SIP à l'aide de la fonction DoS SIP
- Configurer, bloquer et signaler l'utilisation abusive des services et des ports du système à l'aide de la fonction Port Misuse (utilisation abusive des ports)

contre plusieurs types de vecteurs d'attaque.

- Configurer la détection et l'atténuation DoS par profil pour protéger des applications spécifiques contre les attaques.
- Utiliser les signatures dynamiques DoS pour protéger automatiquement le système contre les attaques DoS basées sur des modèles de trafic et de charge de ressources à long terme.
- Construire et configurer des règles de pare-feu réseau à l'aide de BIG-IP iRules
- Être en mesure de surveiller et d'effectuer un dépannage initial des diverses fonctionnalités AFM

## Pré-requis:

Les étudiants doivent avoir suivi l'un des prérequis F5 suivants avant de participer à ce cours :

- Avoir suivi le cours ENW_BIG-IP Administration de BI-IP - Administering BIG-IP (ILT)
- Posséder une certification F5 Certified BIG-IP Administrator

Il est recommandé d'avoir des connaissances et une expérience générales en matière de technologie réseau, y compris l'encapsulation du modèle OSI, le routage et la commutation, Ethernet et ARP, les concepts TCP/IP, l'adressage IP et le sous-réseau, le NAT et l'adressage IP privé, le NAT et l'adressage IP privé, la passerelle par défaut, les pare-feux réseau, et le LAN par rapport au WAN.

## Contenu:

- Configuration and management of the BIG-IP AFM system
- AFM Network Firewall concepts
- Network firewall options and modes
- Network firewall rules, policies, address/port lists, rule lists and schedules
- IP Intelligence facilities of dynamic black and white lists, IP reputation database and dynamic IP shunning.
- Detection and mitigation of DoS attacks
- Event logging of firewall rules and DoS attacks
- Reporting and notification facilities
- DoS Whitelists
- DoS Sweep/Flood
- DNS Firewall and DNS DoS
- SIP DoS
- Port Misuse
- Network Firewall iRules
- Various AFM component troubleshooting commands

## Méthodes pédagogiques :

Un support de cours officiel sera fourni aux participants.
Les cours de formation autodirigée (SDT) gratuits suivants, bien que facultatifs, sont utiles pour tout étudiant ayant une expérience limitée de l'administration et de la configuration de BIG-IP : Commencer avec BIG-IP Commencer avec Local Traffic Manager (LTM) Prise en main de BIG-IP Advanced Firewall Manager (AFM)
Ces modules sont disponibles gratuitement et en anglais sur le site Exclusive Network France via ce lien [F5 Training Programs and Online Classes | F5 ]

## Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement