Formation F5 configuration BIG-IP AFM : Advanced Firewall Manager

F5 Configuring BIGIP AFM: Advanced Firewall Manager

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Ce cours utilise des conférences et des exercices pratiques pour donner aux participants une expérience en temps réel de l'installation et de la configuration du système BIG-IP® Advanced Firewall Manager. Les étudiants sont initiés à l'interface utilisateur AFM, en passant par diverses options qui démontrent comment AFM est configuré pour construire un pare-feu réseau et pour détecter et protéger contre les attaques DoS (déni de service). Les fonctions de rapport et de journal sont également expliquées et utilisées dans les laboratoires du cours. D'autres fonctionnalités de pare-feu et des possibilités supplémentaires de déni de service pour le trafic DNS et SIP sont abordées.

Référence	WGAC-BIG-AFM-CFG
Durée	2 jours (14h)
Tarif	1 900 €HT
Repas	repas inclus

PROCHAINES SESSIONS

Pour connaître les prochaines dates ou organiser un intra-entreprise, contactez-nous, nous vous répondrons sous 72 heures.

Objectifs

| Configurer le pare-feu réseau de l'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 immédiatement les règles de pare-feu ou les tester à l'aide de la mise en scène des règles.
| 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 contre plusieurs types de vecteurs d'attaque.
| Configurer la détection et l'atténuation des dénis de service 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.
| Configurer et utiliser les fonctions de journalisation locale et distante de l'AFM
| Configurer et surveiller l'état de l'AFM à l'aide de diverses fonctions de rapport.
| Exporter les rapports du système AFM vers votre système de surveillance externe, directement ou par courrier programmé.
| Autoriser le trafic choisi à contourner les contrôles DoS à l'aide de listes blanches.
| Isoler les clients potentiellement mauvais des bons à l'aide de la fonction Sweep Flood.
| Isoler et réacheminer le trafic réseau potentiellement mauvais en vue d'une inspection plus approfondie à l'aide de la fonctionnalité IP Intelligence Shun.
| Restreindre et signaler certains types de requêtes DNS à l'aide de la fonction DNS Firewall.
| 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".
| Créer 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 de l'AFM

Public

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

Prérequis

| Avoir suivi "Administration de BIG-IP" (cours avec instructeur) ou F5 Certified BIG-IP Administrator (administrateur certifié de BIG-IP)

Programme de la formation

Configuration et gestion du système BIG-IP AFM
Concepts de pare-feu réseau AFM
Options et modes de pare-feu réseau
Règles de pare-feu réseau, politiques, listes d'adresses et de ports, listes de règles et calendriers
Fonctions de renseignement sur les adresses IP : listes noires et blanches dynamiques, base de données de réputation des adresses IP et exclusion dynamique des adresses IP.
Détection et atténuation des attaques DoS
Enregistrement des règles de pare-feu et des attaques par déni de service.
Fonctions de signalement et de notification
Listes blanches DoS
Balayage/Inondation DoS
Pare-feu DNS et déni de service DNS
DoS SIP
Mauvais usage des ports
Pare-feu réseau iRules
Diverses commandes de dépannage des composants du FAM

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.