Formation F5 - Configuring BIG-IP AFM : Advanced Firewall Manager (AFM)

Objectifs de la formation F5 BIG-IP AFM

Ce cours F5 BIG-IP AFM (Advanced Firewall Manager) donne aux administrateurs de réseau, aux opérateurs de réseau et aux ingénieurs de réseau la possibilité d'acquérir une compréhension fonctionnelle de BIG-IP Advanced Firewall Manager.

À l'issue de cette formation, vous aurez acquis les connaissances nécessaires pour :

- Savoir effectuer l'installation et la configuration du système BIG-IP AF
- Connaître les concepts de firewall réseau AFM
- Utiliser les options et modes de firewall réseau
- Mettre en place des règles, stratégies, listes d'adresses et de ports, listes de règles et renouvellement des adresses IP de listes noires et blanches de façon dynamique et de la base de données du firewall réseau
- Préparer la détection et la prévention des attaques DoS
- Enregistrer des événements des règles de firewall et des attaques DoS
- Connaître les fonctions de déclaration et de notification
- Construire des listes blanches DoS
- Identifier les spécificités des firewalls DNS et DoS DNS
- Aborder DoS SIP et le Firewall réseau iRules
- Connaître diverses commandes de dépannage de composants AFM et configuration du système BIG-IP AFM

La formation se déroule sur la version 14.1 de BIG-IP.

À qui s'adresse cette formation ?

Public :

La formation F5 BIG-IP AFM est destinée aux administrateurs de réseau, aux opérateurs de réseau et aux ingénieurs et architectes réseau responsables de l'installation, de la mise en œuvre, de la configuration et de l'administration du système BIG-IP AFM.

Prérequis :

Les personnes n'ayant jamais utilisé de système F5 doivent suivre au préalable la formation F5 - Administrateur BIG-IP (F101).

Les connaissances et l'expérience suivantes en matière de technologie de réseau sont recommandées avant de participer à ce cours :
Encapsulation du modèle OSI, Routage et commutation, Ethernet et ARP, Concepts TCP/IP, Adressage IP et sous-réseautage, NAT et adressage IP privé, Passerelle par défaut, Pare-feu réseau, LAN vs WAN, Protocoles HTTP et DNS.

Contenu du cours F5 BIG-IP AFM

Chapitre 1 : Mise en place du système BIG-IP

Présentation du système BIG-IP
Configuration initiale du système BIG-IP
Archivage de la configuration du système BIG-IP
Tirer parti des ressources et des outils de soutien F5

Chapitre 2 : Vue d'ensemble de l'AFM et pare-feu réseau

Vue d'ensemble de l'AFM
Disponibilité de l'AFM
AFM et le menu de sécurité BIG-IP
Explication de la terminologie F5
Pare-feu réseau
Contextes

Modes

Traitement des paquets

Règles et directives

Contextes de règles et traitement

Éditeur de règles en ligne

Configuring Network Firewall

Network Firewall Rules and Policies

Création de règles de pare-feu réseau

Identification du trafic par région avec géolocalisation

Identification des règles redondantes et conflictuelles

Identification des règles obsolètes

Pré construction de règles de pare-feu avec des listes et des planifications

Listes de règles

Listes d'adresses

Listes de ports

Horaires

Stratégies de pare-feu réseau

État et gestion de la stratégie

Autres actions de règle

Redirection du trafic avec Envoyer vers le virtuel

Vérification du traitement des règles avec packet tester

Examen des connexions avec Flow Inspector

Chapitre 3 : Journaux

Journaux des événements

Profils de journalisation

Limitation des messages de journal avec la limitation du journal

Activation de la journalisation dans les règles de pare-feu

Mécanismes de journalisation BIG-IP

Éditeur de journaux

Destination du journal

Filtrage des journaux à l'avec la fonction de recherche personnalisée

Journalisation des événements de règle globale

Modifications de la configuration du journal

QKView et fichiers journaux

SNMP MIB

Interruptions SNMP

Chapitre 4 : Renseignements sur la propriété intellectuelle

aperçu

Fonctionnalité 1 Listes dynamiques blanches et noires

Catégories de la liste noire

Listes de flux

Politiques en matière d'intelligence IP

Profil de journal IP Intelligence

Rapports de renseignements sur la PI

Dépannage des listes d'intelligence IP

Fonctionnalité 2 Base de données IP Intelligence

Licences

installation

configuration

dépannage

Ip Intelligence iRule

Chapitre 5 : Protection dos

Vue d'ensemble du déni de service et de la protection DoS

Protection DoS de l'appareil

Configuration de la protection DoS du périphérique

Variante 1 Vecteurs DoS

Variante 2 Vecteurs DoS

Configuration automatique du seuil

Variante 3 Vecteurs DoS

Profils DoS de l'appareil

Profil de protection DoS

Signatures dynamiques

Configuration des signatures dynamiques

DoS iRules

Chapitre 6 : Rapports

Aperçu des installations déclarantes de l'AFM

Examen de l'état des caractéristiques AFM particulières

Exportation des données

Gestion des paramètres de création de rapports

Planification des rapports

Examen de l'état de l'AFM à un niveau élevé

Mini-reporting Windows (Widgets)

Création de widgets personnalisés

Suppression et restauration de widgets

Tableaux

Chapitre 7 : Listes blanches dos

Contournement des contrôles DoS avec des listes blanches

Configuration des listes blanches dos

Options tmsh

Liste d'adresses par profil d'autorisation

Chapitre 8 : DoS Sweep Protection contre les inondations

Isoler les mauvais clients avec Sweep Flood

Configuration de Sweep Flood

Chapitre 9: IP Intelligence Shun

aperçu

Configuration manuelle

Configuration dynamique

Politique en matière de renseignements sur la PI

Options tmsh

Extension de la fonctionnalité Shun

Acheminer ce trafic vers nulle part - Trou noir déclenché à distance

Acheminer ce trafic pour un traitement ultérieur - Scrubber

Chapitre 10 : Pare-feu DNS

Filtrage du trafic DNS avec le pare-feu DNS

Configuration du pare-feu DNS

Types de requêtes DNS

Types d'opcode DNS

Journalisation des événements de pare-feu DNS

dépannage

Chapitre 11 : Dns DoS

aperçu

DNS DoS

Configuration de DNS DoS

Profil de protection DoS

DoS et DNS de l'appareil

Chapitre 12 : SIP DoS

Protocole SIP (Session Initiation Protocol)

Transactions et boîtes de dialogue

SIP DoS Configuration

Profil de protection DoS

DoS et SIP de périphérique

Chapitre 13 : Utilisation abusive des ports

aperçu

Mauvaise utilisation des ports et politiques de service

Création d'une stratégie d'utilisation abusive des ports

Attachement d'une stratégie de service

Création d'un profil de journal

Chapitre 14 : Pare-feu réseau iRules

aperçu

Événements iRule

configuration

Quand utiliser iRules

Plus d'informations

Formation F5

La formation se déroule dans un centre de formation Westcon ATC officiel de F5.