Configuring F5 Advanced WAF (previously licensed as ASM) (TRG-BIG-AWF-CFG)

ID TRG-BIG-AWF-CFG **Prix** US $ 5 280,– (Hors Taxe) **Durée** 4 jours

A qui s'adresse cette formation

Ce cours est destiné aux administrateurs de sécurité et de réseau qui seront responsables de l'installation, du déploiement, de l'optimisation et de la maintenance quotidienne du F5 Advanced Web Application Firewall.

Pré-requis

Les participants doivent valider au moins un de ces pré-requis avant de pouvoir suivre la formation :

- Assister à un cours sur l'administration de BIG-IP (TRG-BIG-OP-ADMIN)
- Obtenir la certification F5 Certified BIG-IP Administrator
- Réussir l'évaluation gratuite de l'équivalence du cours Administering BIG-IP avec un score de 70% ou plus.

Il est recommandé d'avoir les connaissances et l'expérience générales suivantes en matière de technologie réseau avant de participer à un cours dispensé par un instructeur de F5 Global Training Services :

- Encapsulation du modèle OSI
- Routage et commutation
- Ethernet et ARP
- Concepts TCP/IP
- Adressage IP et sous-réseau
- NAT et adressage IP privé
- Passerelle par défaut
- Pare-feu de réseau
- LAN vs. WAN

Objectifs

A l'issue de cette formation, vous serez en mesure de :

- Décrire le rôle du système BIG-IP en tant que proxy complet dans un réseau de distribution d'applications
- Dimensionner le F5 Advanced Web Application Firewall
- Définir un pare-feu d'application Web
- Décrire comment F5 Advanced Web Application Firewall protège une application web en sécurisant les types de fichiers, les URL et les paramètres
- Déployer F5 Advanced Web Application Firewall à l'aide du modèle de déploiement rapide (et d'autres modèles) et définir les contrôles de sécurité inclus dans chacun d'eux
- Définir les paramètres d'apprentissage, d'alarme et de blocage dans le cadre de la configuration de F5 Advanced Web Application Firewall
- Définir les signatures d'attaque et expliquer pourquoi la mise en scène des signatures d'attaque est importante
- Déployer des campagnes de lutte contre les menaces pour se protéger contre les menaces CVE
- Contraster la mise en œuvre de politiques de sécurité positives et négatives et expliquer les avantages de chacune d'entre elles
- Configurer le traitement de la sécurité au niveau des paramètres d'une application Web
- Déployer F5 Advanced Web Application Firewall à l'aide de l'éditeur de politique automatique
- Ajuster une politique manuellement ou permettre l'élaboration automatique d'une politique
- Intégrer les résultats d'un scanner de vulnérabilité d'application tiers dans une politique de sécurité
- Configurer l'application de la connexion pour le contrôle du flux
- Atténuer le bourrage d'informations d'identification (credential stuffing)
- Configurer la protection contre les attaques par force brute
- Déploiement d'une défense avancée contre les robots racleurs de sites web, tous les robots connus et d'autres agents automatisés
- Déployer DataSafe pour sécuriser les données côté client

Contenu

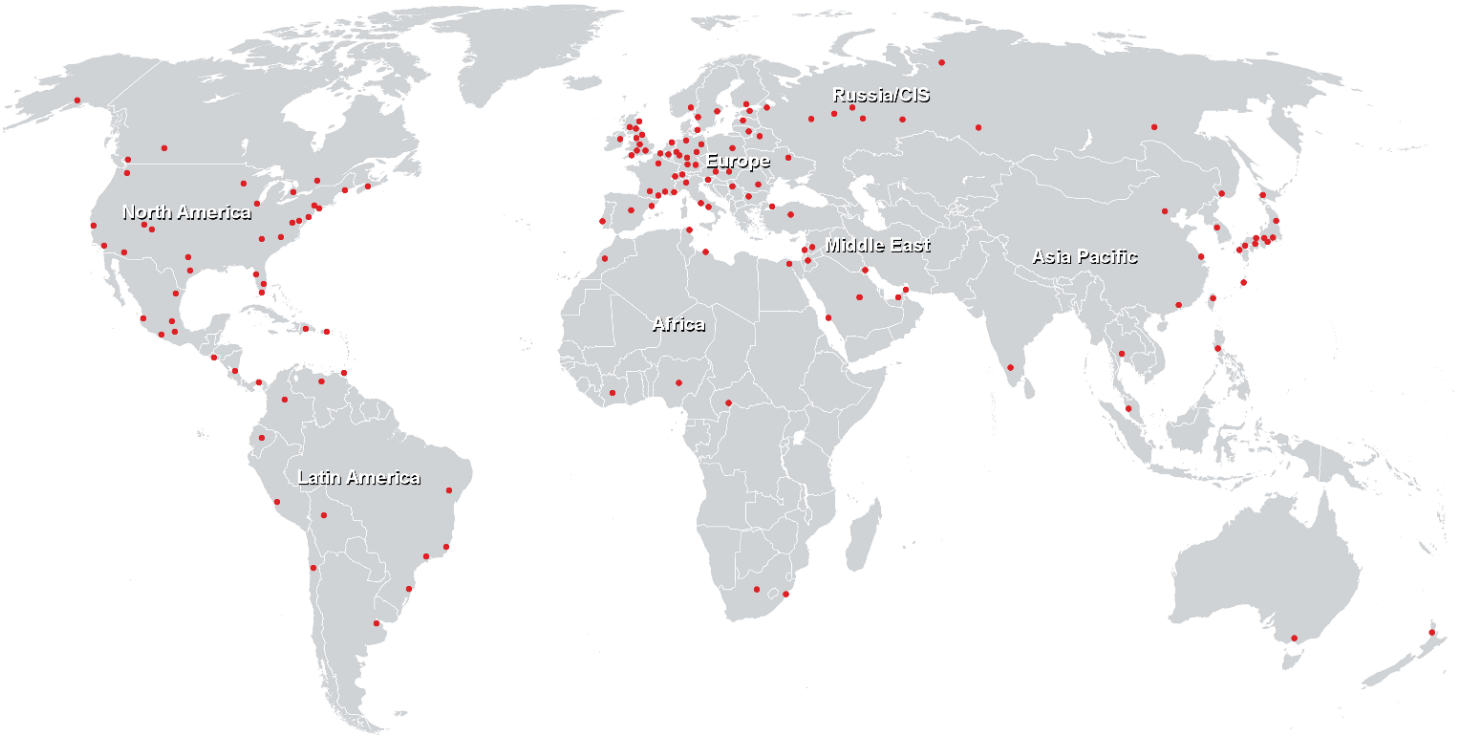
- Provisionnement des ressources pour F5 Advanced Web Application Firewall
- Traitement du trafic avec BIG-IP Local Traffic Manager (LTM)
- Concepts d'application Web
- Atténuation du Top 10 de l'OWASP et d'autres vulnérabilités

Configuring F5 Advanced WAF (previously licensed as ASM) (TRG-BIG-AWF-CFG)

- Déploiement de la politique de sécurité
- Optimisation des politiques de sécurité
- Déploiement de signatures d'attaques et de campagnes de menaces
- Renforcement de la sécurité positive
- Sécurisation des cookies et autres en-têtes
- Rapports et journalisation
- Gestion avancée des paramètres
- Utilisation de l'élaboration automatique de politiques
- Intégration avec des scanners de vulnérabilité web
- Application des règles de connexion pour le contrôle des flux
- Atténuation de la force brute et du bourrage d'informations d'identification
- Suivi de session pour la reconnaissance du client
- Utilisation des politiques parent et enfant
- Protection DoS de la couche 7
- Protection contre les attaques par déni de service basée sur les transactions par seconde
- Protection contre les dénis de service comportementaux de la couche 7
- Configuration d'une défense avancée contre les robots
- Web Scraping et autres protections des microservices
- Travailler avec des signatures de robots
- Utiliser DataSafe pour sécuriser le côté client du Document Object Model
- Certification

Configuring F5 Advanced WAF (previously licensed as ASM) (TRG-BIG-AWF-CFG)

Centres de formation dans le monde entier





Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch