Configuring BIG-IP AFM: Advanced Firewall Manager (TRG-BIG-AFM-CFG)

ID TRG-BIG-AFM-CFG **Preis** US$ 2'200.– (exkl. MwSt.) **Dauer** 2 Tage

Zielgruppe

Dieser Kurs richtet sich an System- und Netzwerkadministratoren, die für die Konfiguration und laufende Verwaltung eines BIG-IP Advanced Firewall Manager (AFM)-Systems verantwortlich sind.

Voraussetzungen

Die Teilnehmer müssen vor diesem Kurs einen der folgenden F5-Kurse absolvieren:

- Präsenzkurs zur Verwaltung von BIG-IP

oder

- F5-zertifizierter BIG-IP-Administrator

Die folgenden kostenlosen, webbasierten Kurse sind zwar freiwillig, aber sehr hilfreich für alle Teilnehmer mit begrenzter BIG-IP-Administrations- und Konfigurationserfahrung.

- Webbasierte Schulung zum Thema Erste Schritte mit BIG-IP
- Webbasierte Schulung zum Thema Erste Schritte mit dem BIG-IP Local Traffic Manager (LTM)
- Webbasierte Schulung zum Thema Erste Schritte mit dem BIG-IP Advanced Firewall Manager (AFM)

Die folgenden allgemeinen Kenntnisse und Erfahrungen auf dem Gebiet der Netzwerktechnologie werden vor der Teilnahme an einem Präsenzkurs von F5 Global Training Services empfohlen:

- OSI-Modell-Kapselung
- Routing und Switching
- Ethernet und ARP
- TCP/IP-Konzepte
- IP-Adressen und Subnetze
- NAT und private IP-Adressen
- Standard-Gateway
- Netzwerk-Firewalls
- LAN vs. WAN

Die folgenden kursspezifischen Kenntnisse und Erfahrungen werden vor der Teilnahme an diesem Kurs empfohlen:

- HTTP- und DNS-Protokolle

Kursziele

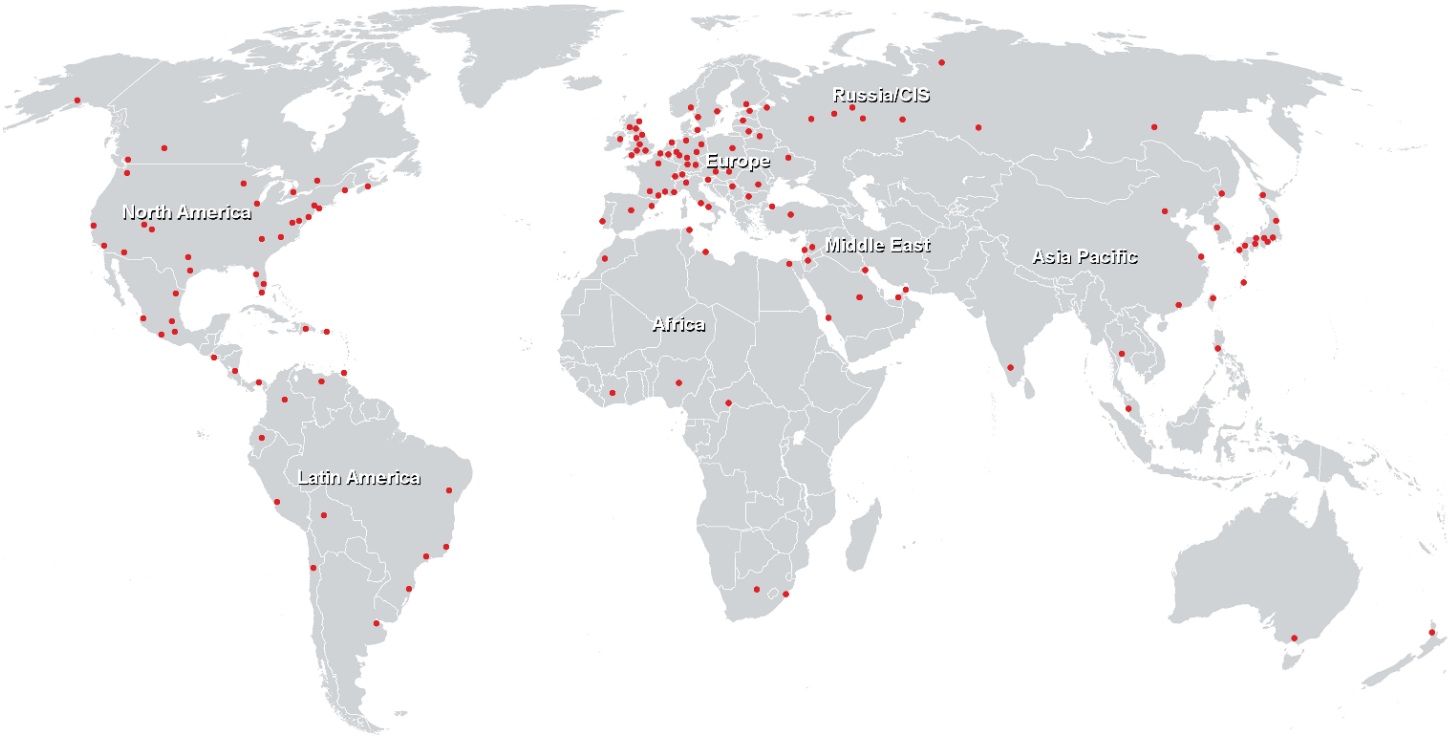
- Konfiguration und Verwaltung eines AFM-Systems
- Konfiguration der AFM-Netzwerk-Firewall in einem positiven oder negativen Sicherheitsmodell
- Konfiguration der Netzwerk-Firewall, sodass Datenverkehr des Netzwerks anhand von Regeln auf der Basis von Protokoll, Quelle, Ziel, Standort und anderen Eigenschaften zugelassen oder blockiert wird
- Vorfertigung von Firewall-Regeln mithilfe von Listen und Zeitplänen
- Sofortige Umsetzung von Firewall-Regeln oder Tests mithilfe des Richtlinien-Stagings
- Verwenden der Funktionen Packet Tester und Flow Inspector, um Netzwerkverbindungen anhand Ihrer Sicherheitskonfigurationen auf Netzwerk-Firewall-, IP-Informations- und DoS-Funktionen zu überprüfen
- Konfiguration verschiedener IP-Informationsfunktionen, um den Zugriff nach IP-Adresse zu identifizieren, aufzuzeichnen, zu erlauben oder zu blockieren
- Konfiguration der Geräte-DoS-Erkennungs- und Abwehrfunktion, um das BIG-IP-Gerät sowie alle Anwendungen vor verschiedenen Arten von Angriffsvektoren zu schützen
- Konfiguration der DoS-Erkennung und -Abwehr auf einer profilweisen Basis, um entsprechende Anwendungen vor Angriffen zu schützen
- Verwenden von dynamischen DoS-Signaturen zum automatischen Schutz des Systems vor DoS-Angriffen auf der Grundlage langfristiger Verkehrs- und Ressourcenauslastungsmuster
- Konfiguration und Verwendung der lokalen und Remote-AFM-Protokollierungsmöglichkeiten
- Konfiguration und Überwachung des AFM-Status mit verschiedenen Berichtsmöglichkeiten
- Direkter Export der AFM-Systemberichte an Ihr externes Überwachungssystem oder über planmässige Nachrichten
- Whitelisting, damit ausgewählter Datenverkehr die DoS-

Prüfungen umgehen kann
- Isolation potenziell bösartiger Clients von legitimen Clients mithilfe der Funktion Sweep Flood
- Isolation und Umleitung von potenziell bösartigem Datenverkehr im Netzwerk zur weiteren Untersuchung mithilfe der Funktion IP Intelligence Shun
- Einschränkung und Meldung bestimmter Arten von DNS-Anfragen mithilfe der DNS-Firewall
- Konfiguration, Abwehr und Meldung DNS-basierter DoS-Angriffe mithilfe der DNS-DoS-Funktion
- Konfiguration, Abwehr und Meldung SIP-basierter DoS-Angriffe mithilfe der SIP-DoS-Funktion
- Konfiguration, Blockierung und Meldung der Ausnutzung von Systemdiensten und Ports mithilfe der Funktion Port Misuse
- Erstellen und Konfigurieren von Netzwerk-Firewall-Regeln mit BIG-IP iRules
- Überwachung und grundlegende Fehlerbehebung verschiedener AFM-Funktionen

Kursinhalt

- Konfiguration und Verwaltung des BIG-IP AFM-Systems
- Konzepte der AFM-Netzwerk-Firewall
- Optionen und Modi der Netzwerk-Firewall
- Regeln, Richtlinien, Adress-/Portlisten, Regellisten und Zeitpläne der Netzwerk-Firewall
- IP-Informationsfunktionen mit dynamischem Black- und Whitelisting, IP-Reputation-Datenbank und dynamischem IP-Shunning.
- Erkennung und Abwehr von DoS-Angriffen
- Ereignisprotokollierung von Firewall-Regeln und DoS-Angriffen
- Berichts- und Benachrichtigungsmöglichkeiten
- DoS-Whitelisting
- DoS-Sweep/-Flood
- DNS-Firewall und DNS-DoS
- SIP-DoS
- Ausnutzung von Ports
- iRules für die Netzwerk-Firewall
- Verschiedene Fehlerbehebungsbefehle für AFM-Komponenten

Weltweite Trainingscenter



Fast Lane Institute for Knowledge Transfer GmbH

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

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