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

ID TRG-BIG-AFM-CFG **Preis** US$ 1.995,– (exkl. MwSt.) **Dauer** 2 Tage

Kursüberblick

Dieser Kurs kombiniert Vorträge und praktische Übungen, um den Teilnehmern in Echtzeit Erfahrungen beim Einrichten und Konfigurieren des BIG-IP Advanced Firewall Manager (AFM)-Systems zu vermitteln. Die Teilnehmer werden in die AFM-Benutzeroberfläche eingeführt und durch verschiedene Optionen geführt, die zeigen, wie AFM konfiguriert wird, um eine Netzwerk-Firewall aufzubauen und Denial-of-Service (DoS)-Angriffe zu erkennen sowie abzuwehren. Die Berichts- und Protokollierungsmöglichkeiten werden ebenfalls erläutert und in den Kurslaboren genutzt. Außerdem werden weitere Firewall-Funktionen und zusätzliche DoS-Einrichtungen für DNS- und SIP-Datenverkehr besprochen.

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

Detaillierter Kursinhalt

Kapitel 1: Einrichtung des BIG-IP-Systems

- Einführung in das BIG-IP-System
- Erstmalige Einrichtung des BIG-IP-Systems
- Archivierung der BIG-IP-Systemkonfiguration
- Nutzung der F5-Hilfsressourcen und -Tools

Kapitel 2: Überblick über AFM

- Überblick über AFM
- Verfügbarkeit von AFM
- AFM und das BIG-IP-Sicherheitsmenü

Kapitel 3: Netzwerk-Firewall

- AFM-Firewalls
- Kontexte
- Modi
- Paketverarbeitung
- Regeln und Weiterleitung
- Kontexte und Verarbeitung von Regeln
- Inline-Regeleditor
- Konfiguration der Netzwerk-Firewall
- Regeln und Richtlinien für Netzwerk-Firewalls
- Erstellung von Regeln für die Netzwerk-Firewall
- Identifizierung des Datenverkehrs nach Region mithilfe der Geolokalisierung
- Identifizierung redundanter und widersprüchlicher Regeln
- Identifizierung veralteter Regeln
- Erstellen von Firewall-Regeln mit Listen und Zeitplänen
- Regellisten
- Adresslisten
- Portlisten
- Zeitpläne
- Richtlinien für die Netzwerk-Firewall
- Policy-Status und -Verwaltung
- Sonstige Regelaktionen
- Umleitung des Datenverkehrs mit Send to Virtual
- Prüfung der Regelverarbeitung mit dem Packet Tester
- Untersuchung von Verbindungen mit dem Flow Inspector

Kapitel 4: Protokolle

- Ereignisprotokolle
- Protokollierungsprofile
- Begrenzung von Protokollmeldungen mithilfe der Protokolleinschränkung
- Aktivierung der Protokollierung in Firewall-Regeln
- BIG-IP-Protokollierungsmechanismen
- Herausgeber des Protokolls
- Ziel des Protokolls
- Filtern von Protokollen mit der benutzerdefinierten Suchfunktion
- Protokollierung globaler Regelereignisse
- Protokollkonfigurationsänderungen
- QKView- und Protokolldateien
- SNMP-MIB
- SNMP-Traps

Kapitel 5: IP-Informationen

- Übersicht
- IP-Informationsrichtlinien
- Funktion 1 Dynamische Positiv- und Negativlisten
- Kategorien der Negativliste
- Feed-Listen
- Anwendung einer IP-Informationsrichtlinie
- IP-Informations-Protokollprofil
- IP-Informationsberichte
- Fehlerbehebung bei IP-Informationslisten
- Funktion 2 IP-Informationsdatenbank
- Lizenzierung
- Installation
- Verknüpfung der Datenbank mit der IP-Informationsrichtlinie
- Fehlerbehebung
- IP-Informations-iRule

Kapitel 6: DoS-Schutz

- Überblick über Denial-of-Service und DoS-Schutz
- DoS-Schutz von Geräten
- Konfiguration des DoS-Schutzes von Geräten
- Variante 1 DoS-Vektoren
- Variante 2 DoS-Vektoren
- Automatische Konfiguration oder automatische Schwellenwerte
- Variante 3 DoS-Vektoren
- DoS-Profile von Geräten
- DoS-Schutzprofil
- Dynamische Signaturen
- Konfiguration von dynamischen Signaturen
- DoS-iRules

Kapitel 7: Berichte

- Überblick über die AFM-Berichtsmöglichkeiten
- Untersuchung des Status bestimmter AFM-Funktionen
- Datenexport
- Verwaltung der Berichtseinstellungen
- Planung von Berichten
- Fehlerbehebung bei der Planung von Berichten
- Umfassende Untersuchung des AFM-Status

- Mini-Berichtsfenster (Widgets)
- Erstellen benutzerdefinierter Widgets
- Löschen und Wiederherstellen von Widgets
- Dashboards

Kapitel 8: DoS-Positivlisten

- Umgehung von DoS-Prüfungen mit Positivlisten
- Konfiguration von DoS-Positivlisten
- tmsh-Optionen
- Profilweise Positiv-Adressliste

Kapitel 9: DoS-Sweep-Flood-Schutz

- Isolation bösartiger Clients mithilfe von Sweep Flood
- Konfiguration von Sweep Flood

Kapitel 10: IP-Informations-Shun

- Übersicht
- Manuelle Konfiguration
- Dynamische Konfiguration
- IP-Informationsrichtlinien
- tmsh-Optionen
- Fehlerbehebung
- Erweiterung der Shun-Funktion
- Routing von Datenverkehr ins Nichts – Fernausgelöstes Schwarzes Loch
- Routing von Datenverkehr zur Weiterverarbeitung – Bereinigung

Kapitel 11: DNS-Firewall

- Filtern des DNS-Datenverkehrs mithilfe der DNS-Firewall
- Konfiguration der DNS-Firewall
- DNS-Anfragetypen
- DNS-OpCode-Typen
- Protokollierung von DNS-Firewall-Ereignissen
- Fehlerbehebung

Kapitel 12: DNS-DoS

- Übersicht
- DNS-DoS
- Konfiguration von DNS-DoS
- DoS-Schutzprofil
- DoS und DNS von Geräten

Kapitel 13: SIP-DoS

- Session Initiation Protocol (SIP)
- Transaktionen und Dialoge
- SIP-DoS-Konfiguration
- DoS-Schutzprofil
- DoS und SIP von Geräten

Kapitel 14: Ausnutzung von Ports

- Übersicht
- Portausnutzung und Servicerichtlinien
- Erstellen einer Portausnutzungs-Richtlinie
- Anfügen einer Servicerichtlinie
- Erstellen eines Protokollprofils

Kapitel 15: Netzwerk-Firewall-iRules

- Übersicht
- iRule-Ereignisse
- Konfiguration
- Zeitpunkt der Anwendung von iRules
- Weitere Informationen

Kapitel 16: Zusammenfassung

- BIG-IP-Architektur und Datenverkehrsfluss
- Überblick über die Verarbeitung von AFM-Paketen

Kapitel 17: Zusatzausbildung und -zertifizierung

- Webbasierte Schulungsreihe zu den ersten Schritten
- Schulungsplan des F5-Präsenzkurses
- F5-Expertenertifizierungsprogramm

Über Fast Lane

Die weltweite Fast Lane-Gruppe ist Spezialist für Technologie- und Business-Training und Beratung im Highend-Bereich. Fast Lane ist autorisierter Trainingspartner führender Hersteller und bietet zudem eigene IT-Trainingsprogramme zu aktuellen Technologien und den wesentlichen Trends an. Herstellerübergreifende Beratungsleistungen reichen von vorbereitenden Analysen und Evaluierungen über die Konzipierung zukunftsweisender IT-Lösungen bis zum Projektmanagement und zur Umsetzung der Konzepte im Unternehmen Training-on-the-Job und Weiterqualifizierung der zuständigen Spezialisten bei den Kunden verbinden die Kernbereiche der Fast Lane Dienstleistungen Training und Consulting.

Fast Lane Services

- ✓ Highend-Technologietraining
- ✓ Business- & Softskill-Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digitale Lernlösungen
- ✓ Content-Entwicklung
- ✓ Remote Labs
- ✓ Talentprogramme
- ✓ Eventmanagement-Services

Trainingsmethoden

- ✓ Klassenraumtraining
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Klassenraum und ILO kombiniert
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobiles Lernen

Technologien und Lösungen

- ✓ Digitale Transformation
- ✓ Artificial Intelligence (AI)
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center

Weltweit vertreten
mit High-End-Trainingszentren in 60 Ländern rund um den Globus

Mehrfach ausgezeichnet
von Herstellern wie AWS, Microsoft, Cisco, Google, NetApp, VMware

Praxiserfahrene Experten
mit insgesamt mehr als 19.000 Zertifizierungen

Deutschland
Fast Lane Institute for Knowledge Transfer GmbH
Tel. +49 40 25334610
info@flane.de / www.flane.de

Österreich
ITLS GmbH
(ITLS ist ein Partner von Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

Schweiz
Fast Lane Institute for Knowledge Transfer (Switzerland) AG
Tel. +41 44 8325080
info@flane.ch / www.flane.ch