BIG-IP Advanced Firewall Manager

DATENBLATT

Inhalt

Umfassender Schutz von Rechenzentrum, Anwendungen und Netzwerk

Unternehmen sind für die eigene Produktivität und den Kundenzugriff von außen auf Anwendungen angewiesen. Diese Anwendungen sowie die damit verbundenen Rechenzentren werden immer häufiger Ziel versierter, gezielter Angriffe.

F5® BIG-IP® Advanced Firewall Manager™ (AFM) ist eine leistungsstarke, zustandsbehaftete Full-Proxy-Firewall, die Rechenzentren vor Bedrohungen schützt, die über gängige Protokolle wie HTTPS, SMTP, DNS und FTP eingehen. Durch eine Anpassung der Firewall-Richtlinien an die geschützten Anwendungen optimiert BIG-IP AFM deren Bereitstellung, Schutz und Überwachung. Mit seiner hohen Skalierbarkeit, Sicherheit und Unkompliziertheit dient der BIG-IP AFM als Grundlage für die Application Delivery Firewall-Lösung von F5.

Wichtige Vorteile

Anpassung an den Netzwerkbedarf

Decken Sie den Skalierungsbedarf im Rechenzentrum mit einer Lösung, die auf der bewährten TMOS®-Architektur von F5 sowie spezieller Hardware und Virtual Editions basiert.

Full-Proxy-Firewall für maximalen Schutz

Terminieren Sie eingehende Kundenverbindungen, und analysieren Sie sie auf Sicherheitsrisiken, bevor Sie an den Server weitergeleitet werden.

Optimierte Firewall-Bereitstellung

Vereinfachen Sie die Sicherheitskonfiguration mithilfe von Firewall-Richtlinien, die sich an den Anwendungen selbst orientieren – und beschleunigen Sie die Bereitstellung von Anwendungen.

Individuelle Berichte für mehr Transparenz

Protokollieren Sie Ereignisse mit hoher Geschwindigkeit und verwenden Sie individuelle Konfigurationen für einzelne Anwendungen für mehr Flexibilität bei Protokollierungszielen und erfassten Daten.

Prüfung von SSL-Sitzungen

Sorgen Sie für eine vollständige Terminierung von SSL-Verbindungen, um auch verdeckte Angriffsversuche zu erkennen – mit hoher Skalierbarkeit sowie hohem Durchsatz.

Hohe Verfügbarkeit von Anwendungen

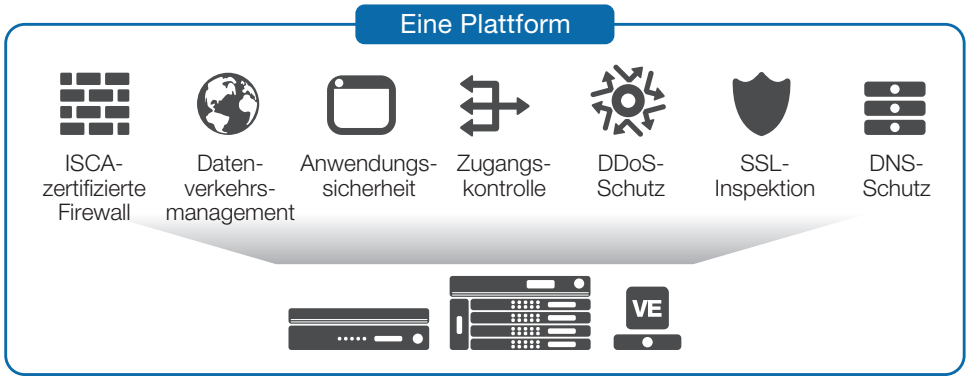
Schützen Sie Netzwerke vor schädlichen IP-Adressen und verhindern Sie DDoS-Angriffe über verschiedene Protokolle mit hardwaregestützter SYN-Flooding-Abwehr. So können Sie die Leistung und Verfügbarkeit spürbar verbessern.

Sicherheit für das anwendungszentrische Netzwerk

Dank umfangreicher Erfahrung in der Entwicklung von Application Delivery-Controllern kann F5 Sicherheit und tiefgehende Einblicke in Anwendungen kombinieren, um Server und Infrastrukturen in Rechenzentren zuverlässig zu schützen.

Application Delivery Firewall

BIG-IP AFM dient als Grundlage für die Application Delivery Firewall-Lösung von F5 und ist das erste Produkt auf dem Markt, das eine Netzwerk-Firewall mit Datenverkehrsmanagement, Anwendungssicherheit, Zugangsverwaltung für Benutzer und DNS-Schutz verbindet. Durch eine Bündelung der Sicherheitsfunktionen verschiedener BIG-IP®-Module auf einer Plattform senkt die Application Delivery Firewall von F5 den Verwaltungsaufwand und bietet zudem unübertroffene Leistung und Skalierbarkeit. Dank BIG-IP® Local Traffic Manager™ verfügt die Application Delivery Firewall über einen tiefgehenden Einblick in gängige Unternehmensanwendungen. Damit ist die Lösung perfekt für den Schutz von öffentlich zugänglichen Anwendungen geeignet – und das unabhängig vom Standort.



Die Application Delivery Firewall von F5 fasst wichtige Netzwerk- und Sicherheitsfunktionen in einer zentralen Plattform zusammen.

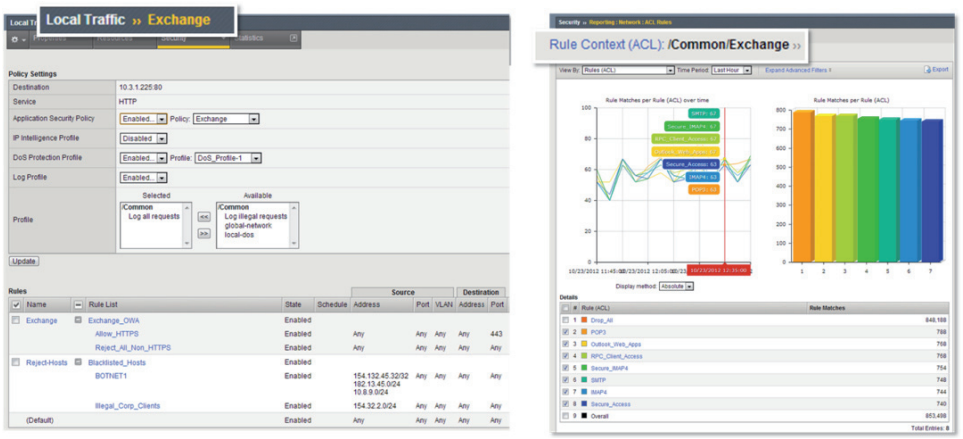
Folgende BIG-IP-Module bilden zusammen eine umfassende Application Delivery Firewall-Lösung:

- BIG-IP Advanced Firewall Manager (AFM) – Diese fortschrittliche Netzwerk-Firewall dient als Grundlage für die Application Delivery Firewall-Lösung von F5. Sie bietet vollständige SSL-Transparenz bei hoher Skalierbarkeit sowie Schutz vor DDoS-Angriffen auf der Netzwerk- und Sitzungsebene.
- BIG-IP Local Traffic Manager (LTM) – Ermöglicht eine verbesserte Verwaltung des Datenverkehrs, Lastverteilung und Anwendungsbereitstellung.
- BIG-IP® Application Security Manager™ (ASM) – Sorgt für Anwendungssicherheit und die Abwehr von Web Scraping, Bots und HTTP-DDoS-Angriffen.
- BIG-IP® Access Policy Manager® (APM) – Übernimmt die Zugangsverwaltung inklusive sicherer Fernzugriffsoptionen und Benutzerkontext.
- BIG-IP® Global Traffic Manager™ (GTM) – Diese skalierbare DNS-Lösung schützt vor DNS-Angriffen wie DDoS und Spoofing. Zudem wird das schnelle Signieren von DNS-Antworten mit DNSSEC unterstützt.
- IP Intelligence and Geolocation – Diese Zusatzdienste stellen Informationen zur Reputation und zum geografischen Standort von IP-Adressen bereit und sorgen so für kontextorientierte Sicherheit.

Anwendungsbezogene Firewall-Regeln

Durch die Kombination von Anwendungsbereitstellung, Anwendungssicherheit, Benutzerzugriff und Firewall-Richtlinien erhöht BIG-IP AFM die Effektivität und vereinfacht die Durchsetzung von Firewall-Richtlinien. Anstelle von starren Lösungen, die sich strikt an Zonen oder Segmenten orientieren, werden Firewall-Richtlinien von BIG-IP AFM logisch auf die Anwendungen selbst abgestimmt. Anwendungsparameter wie Serveradressen, SSL-Offloading und Zugangsrichtlinien werden mit Sicherheitsparametern wie Firewall-Richtlinien, SSL-Inspektion und Protokollierung verbunden. Eine Zuordnung von Anwendungen zu Zonen oder das mühsame Durchsuchen von Tabellen mit Firewall-Richtlinien zum Auffinden der IP-Adresse eines bestimmten Anwendungsservers gehören damit der Vergangenheit an.

Da die Konfiguration einer Anwendung mit der zugehörigen Firewall-Richtlinie verknüpft ist, wird auch die Stilllegung von Anwendungen vereinfacht. Beim Entfernen einer Anwendung werden gleichzeitig auch die damit verbundenen Firewall-Regeln deaktiviert.



BIG-IP AFM stimmt Firewall-Richtlinien auf die Anwendung selbst ab und rationalisiert so für besseren Schutz.

Sicherheit durch Full-Proxy-Firewall

Im Gegensatz zu herkömmlichen Firewalls beruht BIG-IP AFM auf einer Full-Proxy-Architektur: Eingehende Client-Verbindungen werden vollständig terminiert, auf mögliche Sicherheitsbedrohungen untersucht und erst dann an den Server weitergeleitet – natürlich nur, wenn keine Bedrohungen vorliegen.

Umgekehrt fungiert BIG-IP AFM bei der Server-to-Client-Kommunikation ebenfalls als Proxy. So kann die Application Delivery Firewall-Lösung von F5 zurückgesandte Daten auf vertrauliche Informationen analysieren. Dazu zählen beispielsweise Protokollantwortcodes, die Netzwerkdetails für Ausspähversuche oder vertrauliche Daten wie Kreditkarten- und Versicherungsnummern enthalten könnten.

Schutz des Netzwerks vor DDoS-Angriffen

Mit der Full-Proxy-Architektur von BIG-IP AFM ist es möglich, DoS- und DDoS-Angriffe abzuwehren, bevor diese die Server im Rechenzentrum erreichen. So können Sie Ihre Infrastruktur zuverlässig schützen. Zu den sofort einsatzbereiten Funktionen gehört ein umfassender Satz überwachter Bedrohungsvektoren, mit denen Unternehmen viele bekannte DDoS-Angriffe auf ihr Netzwerk abwehren, verfolgen und melden können. Mit DoS-Profilen führt BIG-IP AFM verschiedene Prüfungen durch und wehrt zahlreiche Angriffsformen (wie Flood, Sweep, Teardrop und Smurf) ab. Außerdem werden Protokolle wie SIP und DNS geschützt.

Herausragender DDoS-Schutz

BIG-IP AFM sorgt mithilfe von über 100 DDoS-Vektoren und mehr hardwaregestützten Signaturen als jede andere Firewall-Lösung für sofortigen Schutz vor Bedrohungen. Zudem baut die Lösung auf einer extrem flexiblen Hardwareplattform auf, sodass die vorgegebene Dienstgüte (Quality of Service, QoS) auch bei großen Angriffen gewährleistet bleibt.

BIG-IP AFM bietet mehr Detailgenauigkeit und Transparenz für Datenverkehr und DDoS-Angriffe als andere Lösungen. So können Sie umfassende Protokolle und Berichte für die Erkennung und Abwehr von Angriffen nutzen. Außerdem zeichnet sich die Lösung durch verbesserten Schutz mit SYN-Cookies aus und stellt detaillierte, serverspezifische DDoS-Richtlinien sowie Whitelists und Blacklists bereit. Zur Abwehr groß angelegter, gezielter Flooding-Angriffe kann BIG-IP AFM auf hardwaregestützten DDoS-Schutz zurückgreifen, der auch Angriffe mit großem Volumen abwehrt. So kann legitimer Datenverkehr an sein Ziel gelangen, während DDoS-Attacken ohne Leistungseinbußen abgewiesen werden.

Branchenführender Schutz vor Zero-Day-Angriffen und Erweiterbarkeit

Alle BIG-IP-Module können die Möglichkeiten und die Erweiterbarkeit von F5 iRules® nutzen. Hierbei handelt es sich um eine Skriptsprache mit offenen APIs, die den Inhalt von Datenpaketen direkt auf der Datenebene analysieren kann. Mit iRules können Benutzer individuelle Regeln erstellen, um komplexe Zero-Day-Angriffe abzuwehren. iRules-Befehle sorgen für vollständig transparente Pakete (inklusive der Felder von IP/TCP-Headern), sodass mit iRules-Signaturen eine effektive Flusskontrolle und L2- bis L4-DDoS-Signaturen möglich werden. Durch eine Anpassung mit iRules lassen sich auch Funktionen wie IP Intelligence, Geolocation und statistische Stichproben nutzen. F5 DevCentral™ ist eine Community mit über 120.000 F5-Benutzern, in der Unternehmen iRules mit anderen austauschen können. So erhalten Administratoren die Möglichkeit, die Leistungsmerkmale von BIG-IP AFM flexibel zu erweitern.

Zentrale Verwaltung von Firewall-Richtlinien

In vielen Unternehmen, die verschiedene BIG-IP AFM- und BIG-IP ASM-Geräte zum Schutz einsetzen, kann F5 BIG-IQ® Security die Verwaltung von Firewall-Regeln erleichtern. So steht eine zentrale Verwaltungsoberfläche und einheitliche Übersicht für Sicherheitsregeln verschiedener BIG-IP AFM- und BIG-IP ASM-Geräte zur Verfügung. BIG-IQ Security bietet eine hochgradig skalierbare und erweiterbare Lösung für die Verwaltung von Firewall-Richtlinien und Konfigurationselementen in der gesamten BIG-IP-Sicherheitsinfrastruktur und vereinfacht die Erstellung, Modifizierung, Bereitstellung und Verwaltung von Richtlinien.

Schutz für Service Provider

BIG-IP AFM ist dank exzellenter Skalierbarkeit und Leistung auch perfekt für Cloud- und Kommunikationsumgebungen von Service Providern geeignet. Bei Service Providern sorgt BIG-IP AFM für hohe Leistung, da die Lösung nicht nur das Netzwerk, sondern auch Kunden vor Angriffen schützt.

In mobilen Netzwerken dient BIG-IP AFM als Grundlage für die S/Gi-Firewall-Lösung von F5. Die S/Gi-Firewall-Lösung wird an der Gi-Schnittstelle von 3G-Netzwerken und der SGi-Schnittstelle von 4G-/LTE-Netzwerken bereitgestellt und sorgt für den Schutz des Netzwerkperimeters, der Mobilitätsinfrastruktur sowie der Mobilfunkkunden. Außerdem bietet die Lösung Service Providern ausreichend Skalierbarkeit und Flexibilität für die Durchsetzung weiterer Services.

Die S/Gi-Firewall-Lösung nutzt das intelligente Service-Framework von F5, damit Kommunikationsanbieter zusätzliche Netzwerk- und Sicherheitsfunktionen wie NAT der Carrier-Klasse und transparenten Kunden-Datenverkehr auf einer Plattform zusammenfassen können.

Mit BIG-IP AFM mit F5 Scale-N™ Virtual Clustered Multiprocessing™-Systemen (vCMP) profitieren Cloud- und Kommunikationsanbieter von dem kosteneffektivsten Ansatz für die Verwaltung großer Firewall-Umgebungen. Mit vCMP können Administratoren bequem verschiedene Firewalls auf einem Gerät zusammenführen und BIG-IP AFM-Ressourcen flexibel und für verschiedene Kunden, Gruppen, Anwendungen und Services getrennt bereitstellen. Zudem unterstützt vCMP eine Isolierung von High-Density-Firewalls sowie das Clustering von Gast-Firewalls, um die Verwaltung und Pflege zu vereinfachen und in der ganzen Firewall-Infrastruktur für Konsistenz zu sorgen.

BIG-IP AFM – Leistungsmerkmale und technische Daten

BIG-IP Advanced Firewall Manager ist eine zustandsbehaftete Full-Proxy-Firewall für erweiterten Netzwerkschutz.

Firewall

Erkennung von Protokollanomalien	Ja – SYN/ICMP/ACK/UDP/TCP/IP**/DNS/ARP
L4-DoS- und DDoS-Schutz	Ja
SSL-DoS- und DDoS-Schutz	Ja
DoS- und DDoS-Schutz	Ja
HTTP-DoS- und DDoS-Schutz	Ja
SSL-Reverse-Proxy	Ja
IP-Reputation* und geografische Herkunft	Ja – inklusive Erkennung von Tor-Proxys, Malware und Command-and-Control-Servern (C&C)
Zentrale Verwaltung mit rollen-abhängiger Zugangskontrolle	Ja – mit BIG-IQ Security
SNMP-Reporting	Ja
Stichproben für DDoS-Datenverkehr	Ja

* Separate Lizenzierung
** Unterstützung für IPv4 und IPV6

IPsec

Site-to-Site	Ja
Schlüsselmethoden	Manuell, Internet Key Exchange (IKEv1 und IKEv2)
Authentifizierungsmethoden	Preshared Key, RSA-Signatur
Diffie-Hellman-Gruppen	1, 2, 5, 14, 15, 16, 17, 18
Verschlüsselungsalgorithmen	3DES, AES-128, AES-192, AES-256, AES-GCM-128, AES-GCM-256
Hash-/HMAC-Algorithmen	SHA-1, AES-GMAC-128, AES-GMAC-192, AES-GMAC-256

Plattformmerkmale

Mandantenfähigkeit	Ja – mit vCMP
Hochverfügbarkeit	Ja – aktiv-passiv oder aktiv-aktiv

SSL-VPN

Fernzugriff	Ja – mit BIG-IP APM

Skalierbarkeit und Leistung	VIPRION 4800 (8 × B4340)	VIPRION 4480 (4 × B4300)	VIPRION 2400 (4 × B2100/ B215/B2250)	VIPRION 2200 (2 × B2100/ B215/B2250)
Maximaler Firewall-Durchsatz	640 GBit/s	320 GBit/s	160/160/320 GBit/s	80/80/160 GBit/s
Verbindungen pro Sekunde	7,5 Millionen	4,8 Millionen	1,5 Millionen/ 1,5 Millionen/ 3,8 Millionen	750.000/ 750.000/ 1,9 Millionen
Maximale gleich-zeitige Verbindungen	576 Millionen	144 Millionen	44 Millionen/ 88 Millionen/ 176 Millionen	22 Millionen/ 44 Millionen/ 88 Millionen

Skalierbarkeit und Leistung	BIG-IP 11050s/11000v	BIG-IP 10050s/10250v	BIG-IP 7050s/7250v	BIG-IP 5050s/5250v
Maximaler Firewall-Durchsatz	42 GBit/s bzw. 24 GBit/s	80 GBit/s	40 GBit/s	30 GBit/s
Verbindungen pro Sekunde	900.000	850.000	370.000/ 750.000	330.000/ 670.000
Maximale gleich-zeitige Verbindungen	24 Millionen/ 30 Millionen	36 Millionen	22 Millionen	22 Millionen

Skalierbarkeit und Leistung	BIG-IP 4000s/4200v	BIG-IP 2200s	BIG-IP 2000s
Maximaler Firewall-Durchsatz	10 GBit/s	5 GBit/s	5 GBit/s
Verbindungen pro Sekunde	130.000/ 250.000	135.000	67.000
Maximale gleich-zeitige Verbindungen	9 Millionen/ 10 Millionen	5 Millionen	4,5 Millionen

BIG-IP AFM – Verfügbarkeit

BIG-IP Advanced Firewall Manager ist zusammen mit anderen Modulen in Form von Paketen erhältlich, um individuelle Anforderungen an Application Delivery Firewalls zu unterstützen. Dazu gehören:

Name des Pakets	BIG-IP AFM	BIG-IP LTM	BIG-IP ASM	BIG-IP APM	BIG-IP APM Lite (10 Benutzer)
Application Delivery Firewall	✓	✓			✓
Application Delivery Firewall mit Application Security	✓	✓	✓		✓
Application Delivery Firewall mit Access Management	✓	✓		✓	✓
Application Delivery Firewall mit Application Security und Access Management	✓	✓	✓	✓	✓
Advanced Firewall Manager-Add-On (für Systeme, auf denen bereits BIG-IP LTM genutzt wird)	✓				

Hinweis: Alle BIG-IP AFM-Lizenzen umfassen Protokollschutz, Routing und maximale SSL-Sicherheit. IP Intelligence und Geolocation sind für alle Pakete als zusätzliche Add-ons verfügbar.

BIG-IP AFM-Plattformen

BIG-IP Advanced Firewall Manager ist als Add-on-Modul für BIG-IP Local Traffic Manager erhältlich (auf allen BIG-IP-Plattformen). Genaue technische Daten finden Sie im Datenblatt zur BIG IP System-Hardware.

BIG-IP LTM Virtual Edition

Die BIG-IP LTM Virtual Edition (VE) ist eine Version des BIG-IP-Systems, die auf virtuellen Maschinen ausgeführt wird. BIG-IP Advanced Firewall Manager lässt sich als Virtual Edition bereitstellen. BIG-IP VE beinhaltet alle Leistungsmerkmale von BIG-IP-Geräten, die auf dem standardmäßigen TMOS von F5 basieren. Ausnahmen werden in den Versionshinweisen und der Produktdokumentation aufgeführt.

VIPRION-Plattformen

BIG-IP Advanced Firewall Manager ist auch als Add-on-Modul für BIG-IP Local Traffic Manager auf die modulare Plattform F5 VIPRION® erhältlich. Diese Chassis- und Blade-Architektur ist bei wachsenden Application Delivery Networks besonders einfach skalierbar. Weitere Informationen hierzu finden Sie im VIPRION-Datenblatt.

Vereinfachte Lizenzierung

Noch nie war es so einfach, Anwendungen in einer dynamischen Umgebung bereitzustellen. F5 bietet drei Leistungsstufen an, mit denen leistungsstarke Module nach Bedarf und in Abhängigkeit von den jeweiligen Anforderungen eingesetzt werden können: „Good“, „Better“ und „Best“.

- Entscheiden Sie selbst, welche Lösungen für Ihre Anwendungsumgebung am besten geeignet sind – mit den F5-Referenzarchitekturen.
- Stellen Sie mithilfe der F5-Optionen „Good“, „Better“ und „Best“ genau diejenigen Module bereit, die für den Betrieb Ihrer Anwendungen erforderlich sind.
- Schaffen Sie größtmögliche Anwendungsflexibilität, indem Module entweder auf einer virtuellen oder physischen Plattform bereitgestellt werden.

F5 Global Services

F5 Global Services bietet Support, Schulungen und Consulting der Spitzenklasse. So holen Sie das Maximum aus Ihrer Investition in F5 heraus. Sie benötigen schnell eine Antwort auf eine dringende Frage? Sie müssen interne Teams schulen? Oder Sie benötigen Unterstützung bei der Implementierung? F5 Global Services sorgt dafür, dass Ihre Anwendungen stets sicher, schnell und zuverlässig arbeiten. Weitere Informationen zu F5 Global Services finden Sie unter f5.com/services. Persönlich erreichen Sie uns unter der Adresse consulting@f5.com.

Weitere Informationen

Besuchen Sie unsere Website f5.com, um mehr über BIG-IP Advanced Firewall Manager und ergänzende Lösungen zu erfahren. Dort können unter anderem folgende Ressourcen abgerufen werden (in englischer Sprache):

Datenblätter

BIG-IP Application Security Manager
IP Intelligence Services
BIG-IP Access Policy Manger

Webseiten

BIG-IP Advanced Firewall Manager

Lösungsprofil

High-Performance Application Delivery Firewall

Whitepaper

A New Firewall for the Data Center
Mitigating DDoS Attacks

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119, USA; Tel. (+1) 888-882-4447 www.f5.com

F5 Networks, Inc.
Unternehmenszentrale
info@f5.com

F5 Networks Ltd.
Europa/Naher Osten/Afrika
emeainfo@f5.com

F5 Networks GmbH
Lehrer-Wirth-Straße 2
81829 München
Tel. 089 94 383-0
germanyinfo@f5.com

Solutions for an application world.