BIG-IP Advanced Firewall Manager

DATASHEET

目次

データセンターとアプリケーションの保護

企業は社内の生産性の確保と社外の顧客へのアクセスの両方でアプリケーションに依存しています。同時に、アプリケーションとそれらをホスティングするデータセンターでは、高度化・複雑化するDoS攻撃（サービス拒否攻撃）にさらされる機会が増えてきています。

F5® BIG-IP® Advanced Firewall Manager™（AFM）は高性能でステートフルなフルプロキシ型のネットワーク・ファイアウォールであり、HTTP/S、SMTP、DNS、FTPなど、幅広く採用されているプロトコルを使ってこのような外部脅威からデータセンターを保護します。保護対象のアプリケーションに合わせてファイアウォール・ポリシーを設定することで、アプリケーションの導入、セキュリティ、監視を合理化します。BIG-IP AFMの特徴である高度な拡張性と、セキュリティ、シンプルさはF5アプリケーション・デリバリ・ファイアウォール・ソリューションの核となるものです。

主なメリット

ネットワークのニーズに合わせた拡張

F5の独自OSであるTMOS®アーキテクチャ、幅広いハードウェアプラットフォーム、バーチャル・エディションをベースに構築されたソリューションにより、データセンターの厳しい拡張ニーズに対応します。

フルプロキシ・ファイアウォールによる防御

着信クライアント接続がサーバに到達する前にそれらを終端して検査を行い、セキュリティ脅威が含まれていないかどうか調べます。

ファイアウォール導入の合理化

アプリケーション視点のファイアウォール・ポリシーによりセキュリティ設定を簡素化すると同時に、アプリケーションの導入にかかる時間を短縮します。

レポーティングのカスタマイズによる可視化

イベントの高速記録とアプリケーション単位のログ設定により、ログ先と記録情報を柔軟に指定できます。

SSLセッションの検査

隠れた攻撃を見つけ出すためのSSL接続の終端を、高スループットで大規模に実施します。

アプリケーションの安定性の確保

攻撃状況を詳細に把握することで、38のDoS攻撃ベクトルをブロックし、アプリケーションの安定性を確保します。一部のプラットフォームについては、ハードウェアでSYNフラッド防御に対応するようになっています。

ICSA labs CERTIFIED IPSEC

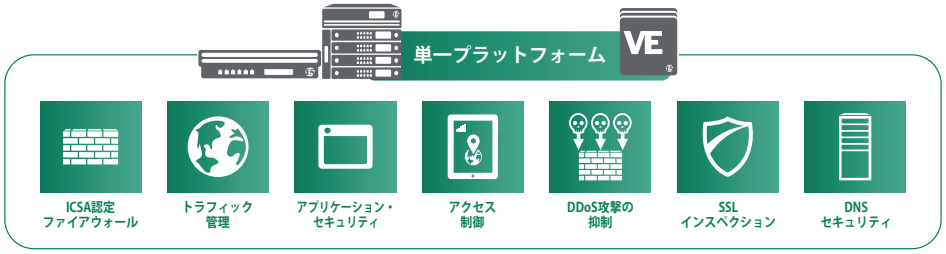
ICSA labs CERTIFIED FIREWALL - CORPORATE

新しいアプリケーション中心型ネットワークのセキュリティ

F5はアプリケーション・デリバリ・コントローラ分野での豊富な経験を活かし、アプリケーション・トラフィックを理解しているF5にしかできないアプローチでサーバとデータセンター・インフラを保護します。

アプリケーション・デリバリ・ファイアウォール

アプリケーション・デリバリ・ファイアウォールとはネットワーク・ファイアウォールとトラフィック管理、アプリケーション・セキュリティ、ユーザアクセス管理、DNSセキュリティを統合したファイアウォール・ソリューションです。複数のBIG-IP®モジュールのセキュリティ機能を1つのプラットフォームに集約することで、高度なパフォーマンスと拡張性はそのままに、管理の複雑さとオーバーヘッドを軽減します。最も豊富な実績を誇るBIG-IP® Local Traffic Manager™をベースに構築された同ファイアウォールは、広く導入されているエンタープライズ・アプリケーションに関する深いアプリケーション・フルエンシを備えています。このことが、アプリケーションに特化した特異な遅延状況の検出など、高度なセキュリティ機能へとつながっています。



F5アプリケーション・デリバリ・ファイアウォールは、ネットワークとセキュリティの重要な機能を1つのプラットフォームに集約します。

以下のBIG-IPモジュールがアプリケーション・デリバリ・ファイアウォール・ソリューションを構成するものです。

- **BIG-IP Advanced Firewall Manager(AFM)** — アプリケーション・デリバリ・ファイアウォール・ソリューションの中核となる高度なネットワーク・ファイアウォールです。SSLの完全な可視化を広範囲で可能にすると同時に、ネットワーク層とセッション層において分散型サービス拒否(DDoS)攻撃を抑制します。
- **BIG-IP Local Traffic Manager(LTM)** — 高度なトラフィック管理、ロードバランシング、アプリケーション・デリバリ機能を提供します。
- **BIG-IP® Application Security Manager™(ASM)** — アプリケーション・セキュリティ、Webスクレイピングとボット防御、HTTP DDoS攻撃の抑制を提供する、F5のWAF製品です。
- **BIG-IP® Access Policy Manager®(APM)** — アクセス管理、セキュアなリモートアクセス、ユーザコンテキストを提供します。
- **BIG-IP® Global Traffic Manager™(GTM)** — DNS DDoSやスプーフィング(なりすまし)などのDNS攻撃を阻止する高拡張なDNSソリューションです。DNSSECを使った高性能なDNS応答署名もあわせて提供します。
- **IPインテリジェンスとジオロケーション** — これらの付加サービスはIPレピュテーションとジオロケーション情報を提供することで、コンテキスト認識型セキュリティを補完します。

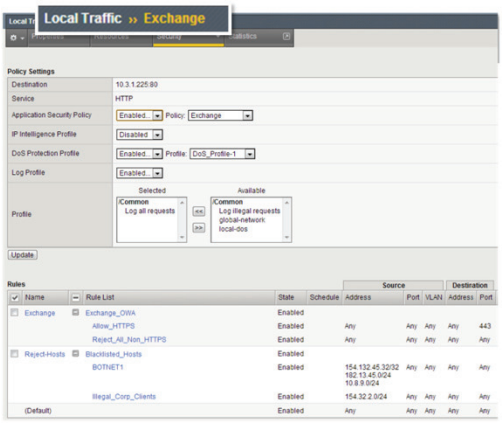
アプリケーション中心型のファイアウォール・ポリシー

BIG-IP AFMは、アプリケーション・デリバリ、アプリケーション・セキュリティ、ユーザアクセス、ファイアウォール・ポリシーを1つに集約することで、アプリケーションの導入を合理化し、ファイアウォール・ポリシーの煩雑化を回避します。

柔軟性に乏しいゾーンベースやセグメントベースの構成と違い、BIG-IP AFMではアプリケーションベースのファイアウォール・ポリシーを設定できます。このことはIT組織にいくつかの運用上のメリットをもたらします。もっとも直接的なメリットとしては、アプリケーション・チームとネットワーク/セキュリティ・チームが今までと違って「アプリケーション視点で構成された同じファイアウォール管理ポリシー」を中心に運用管理などをプランニングでき、効率的な運用体制や計画立案が出来るようになる点です。サーバのアドレス指定、SSLオフロード、アクセスポリシーといったアプリケーション・パラメータの詳細は、現在はセキュリティ・パラメータ（ファイアウォール・ポリシー、SSLインスペクション、ロギングなど）と一緒に分類されています。アプリケーションをゾーンにマッピングしたり、ファイアウォール・ポリシーそのものを別の資料などで管理し、その中で調べて特定のアプリケーション・サーバに適用できるIPアドレスを探したりといった本末転倒で煩雑な管理作業を行っていたのは、もはや過去のことです。

さらには、アプリケーション設定が関連するファイアウォール・ポリシーと統合されているため、アプリケーションのプロビジョニング解除も容易に行えます。アプリケーションのプロビジョニングを解除すると、古いファイアウォール・ルールのプロビジョニングも一緒に解除されます。

BIG-IP AFMはファイアウォール・ポリシーをアプリケーションそのものに合った内容にすることで、セキュリティ・オペレーションを合理化します。



フルプロキシ・セキュリティ

従来型のファイアウォールと違い、BIG-IP AFMはフルプロキシ・アーキテクチャをベースに構築されています。つまり、着信クライアント接続を完全に終端させ、検査を行いセキュリティ脅威が含まれていないことを確認するまでは、接続がサーバに送られることはありません。

逆方向のサーバ-クライアント間の通信も同様にプロキシされ、BIG-IP AFM搭載のF5アプリケーション・デリバリ・ファイアウォール・ソリューションが返信データをスクラビングして機密情報（ネットワーク情報が漏れて偵察攻撃に利用される可能性のあるプロトコル応答コードや、クレジットカード番号や社会保障番号といった個人情報など）を取り除きます。

iRuleを使ったセキュリティの拡張

全てのBIG-IPモジュールでは、データパネル内でペイロードを直接操作できるオープンAPIを使って、F5製品の強みであるプログラミング言語iRulesを活用できます。F5 DevCentral™は10万人以上のF5ユーザで構成されるコミュニティであり、iRuleを開発・共有するための環境をユーザに提供します。管理者はDevCentralを利用して、BIG-IP AFMの機能を柔軟に拡張することが可能です。これまでにDevCentralは、以下のiRuleソリューションをはじめ、数々の重要なセキュリティ機能をお客様に提供してきました。

iRule	ソリューション
透過的なWebアプリボット防御	コンタクトフォームを狙った自動ボットからの不正な要求をブロック
分散型Apacheキラー	Webサーバのサービス拒否（DDoS）の原因となるアプリケーション要求を拒否
iRuleを使ったDNSブラックホール	社員が既知の悪質なWebサイトにアクセスすることをDNSレベルで防止
辞書攻撃の阻止	指数バックオフ・アルゴリズムを利用した過剰なログインを阻止
SSL再ネゴシエーションDoS攻撃	SSLセッションの再交渉を1分間に5回以上繰り返す接続を破棄

BIG-IP AFMの機能と仕様

BIG-IP Advanced Firewall Managerは、高度なネットワーク保護を提供するステートフルなフルプロキシ型のネットワーク・ファイアウォールです。

ファイアウォール	
プロトコル異常検知	あり
L4 DoS&DDoS防御	あり
SSL DoS&DDoS防御	あり
DNS&DDoS防御	BIG-IP GTMを活用する事で実現。
HTTP DoS&DDoS防御	BIG-IP ASMを活用する事で実現。
対応可能なDoS攻撃ベクトル数	38
SSLインスペクション	あり
IPレピュテーションとジオロケーション	あり。IP Intelligence Servicesを活用する事で実現。Tor出口ノード/匿名プロキシ、マルウェア、コマンド&コントロール（C&C）サーバの特定を含む（別途ライセンスが必要）。

カスタムレポートは、情報分析のための詳細なデータと統計を提供します。

IPsec	
サイトツーサイト	あり
鍵交換方式	手動、Internet Key Exchange v1（IKEv1）
認証方式	事前共有鍵、RSA署名
Diffie-Hellmanグループ	1, 2, 5, 14, 15, 16, 17, 18
暗号化アルゴリズム	3DES、AES-128、AES-192、AES-256、AES-GCM-128、AES-GCM-256
ハッシュ/HMACアルゴリズム	SHA-1、AES-GMAC-128、AES-GMAC-192、AES-GMAC-256

プラットフォーム機能

マルチテナンシ	あり。vCMP機能を活用する事で実現。
ハイアベイラビリティ	あり。アクティブ-パッシブまたはアクティブ-アクティブ。

SSL VPN

リモートアクセス	あり。BIG-IP APMを活用する事で実現可能。

規模と性能	VIPRION 4800 （8 x B4300）	VIPRION 4480 （4 x B4300）	VIPRION 2400 （4 x B2100）	BIG-IP 11050/11000	BIG-IP 10200v
最大ファイアウォール・スループット	640Gbps	320Gbps	160Gbps	44Gbps/ 24 Gbps	80Gbps
1秒あたりの接続数	880万	480万	180万	110万	85万
最大同時接続数	2億8,800万	1億4,400万	4,800万	2,400万 /3,000万	3,600万

	BIG-IP 8950/8900	BIG-IP 4200v	BIG-IP 6900	BIG-IP 3900
最大ファイアウォール・スループット	20Gbps/ 12Gbps	10Gbps	6Gbps	4Gbps
1秒あたりの接続数	81万/36万	25万	22万5,000	15万8,000
最大同時接続数	1,200万	1,000万	600万	600万

ビジュアル・ポリシー・エディタでは、アクセスポリシーを簡単に作成できます。

	BIG-IP 2200S	BIG-IP 2000S	BIG-IP 3600	BIG-IP 1600
最大ファイアウォール・スループット	5Gbps	2.5Gbps	2Gbps	1Gbps
1秒あたりの接続数	13万5,000	6万7,000	5万9,000	3万6,000
最大同時接続数	500万	250万	300万	300万

BIG-IP AFMの提供形態について

BIG-IP Advanced Firewall Managerは単体の型番以外に、アプリケーション・デリバリ・ファイアウォールというパッケージの一部としても提供されます。このパッケージングには下記の複数種類あり、各種パッケージに含まれるモジュールの一覧は以下の通りです。

バンドル名	BIG-IP AFM	BIG-IP LTM	BIG-IP ASM	BIG-IP APM
Application Delivery Firewall	✓	✓		
Application Delivery Firewall with Application Security	✓	✓	✓	
Application Delivery Firewall with Access Management	✓	✓		✓
Application Delivery Firewall with Application Security and Access Management	✓	✓	✓	✓
Advanced Firewall Manager Add-On（BIG-IP LTM導入済みのシステム用）	✓			

注：全てのBIG-IP AFMライセンスにはプロトコル・セキュリティ、ルーティング、最大SSLが含まれます。

BIG-IP AFM プラットフォーム

BIG-IP Advanced Firewall Managerは、各種BIG-IP プラットフォームまたはBIG-IP Virtual Edition（VE）でご提供します。提供形態の詳細、対応プラットフォーム、各プラットフォームの物理仕様の詳細については、下記のwebページのBIG-IP システム・ハードウェアスペックシートをご確認下さい。

http://www.f5networks.co.jp/product/spec/index.html

F5 サービス

F5 サービスは、ワールドクラスのサポート、トレーニング、およびコンサルティングによって、F5 に対するお客様の投資効果を最大限に高めます。質問に対するすばやい回答、社内チームのトレーニング、または設計から導入への実装全体への対応など、すべてにおいてF5 サービスはITアジリティの実現を支援します。F5 サービスの詳細については、http://www.f5networks.co.jp/service/ をご覧ください。

F5 ネットワークスジャパン株式会社

東京本社
〒107-0052 東京都港区赤坂 4-15-1 赤坂ガーデンシティ 19 階
TEL 03-5114-3210 FAX 03-5114-3201

西日本支社
〒530-0012 大阪府大阪市北区芝田 1-1-4 阪急ターミナルビル 16 階
TEL 06-7222-3731 FAX 06-7222-3838

www.f5networks.co.jp

CS03-1967 0113