



APPLICATION READY NETWORK GUIDE

SAP

SAP導入時のパフォーマンス、セキュリティ、アベイラビリティを強化する包括的なインフラストラクチャ



概要

SAP®は世界最大手のビジネスソフトウェアを提供する企業です。企業向けソフトウェア・アプリケーションとビジネス・ソリューションを幅広く提供し、ビジネスのあらゆる局面をサポートしています。SAP製品を導入した企業は、その強力なアプリケーションに対して時間的にも資金的にも高額の投資をしています。SAPでテストと認証を受けたF5ネットワークス(以下、F5)のSAP対応Application Readyインフラストラクチャを活用すると、ネットワーク・インフラストラクチャの高速化、セキュリティとアベイラビリティの強化が実現し、運用コストの削減と優れたROIが達成されます。

F5の技術によりSAPに合わせて最適化されたネットワーク・フレームワークを使用することで、企業はサービス品質、管理品質を確保、コンテンツの配信にビジネスポリシーや規定を適用します。また、増大するトラフィック・ボリュームに対応し、使用するアプリケーションを安全に配信しながら、運用効率やコスト管理を改善、今後のアプリケーションやインフラストラクチャの変更に対する柔軟性を維持して投資を保護します。その結果、セキュリティ上の脅威、ネットワークの障害、トラフィックの混雑からの保護と将来的な変化への対応により、優れた操作性とパフォーマンスを実現します。

SAPアプリケーションの配信を最適化し、導入効果を最大化するソリューション、それがApplication Ready Networkです。

メリットとF5の強み

ユーザ価値とアプリケーションのパフォーマンス

SAPのようなアプリケーションのコアスイートを導入するには、慎重な計画と実行が必要です。多くの企業では、アプリケーションを実際に稼働してはじめて、アプリケーションが最適化されていても、ネットワーク・インフラストラクチャによってエンドユーザのアプリケーションのパフォーマンスが低下することに気づきます。企業のIPネットワークは通常Eメール、VoIP、一般的なインターネット・アクセスなど、さまざまなサービスでリソースを共有しています。これらのサービスはネットワークリソースを消費するため、SAPアプリケーションに悪影響を及ぼします。

ネットワークの条件、ITインフラストラクチャの問題またはその他の要因によってアプリケーションのパフォーマンスが低下すると、利用率の低下やビジネスプロセスの遅延などの問題が発生します。ユーザは新しいアプリケーションを目の前にした時点で、すでに変化に対する抵抗を感じています。アプリケーションのパフォーマンスが予測を下回れば、たとえその原因がアプリケーションになかったとしても、利用頻度や利用に対する意欲が減退し、生産性にも悪影響を及ぼします。このようなパフォーマンスの問題は、プロセスの過剰な遅延によってユーザの生産性が低下するだけでなく、一般に利用されているインターネット接続でアプリケーションに直接的または間接的にアクセスする消費者にとっても不満の原因となり、その利用を妨げる可能性があります。F5のApplication Ready NetworkはSAPアプリケーションのネットワークを最適化することで、このようなネットワーク・インフラストラクチャの問題の多くを解決し、最良のユーザ価値を提供します。

Webアプリケーションが遅延すると、多くの場合、まず帯域幅やサーバの容量を増やして対処しますが、それによって根本的な問題、つまり、遅延が解決されるわけではありません。F5ではこの問題を解決するため、ブラウザで繰り返し同じデータをダウンロードするのではなく、ブラウザの動作を制御して、帯域幅の利用を最適化します。この機能により、ブラウザとWebアプリケーション間の冗長な条件付きリクエストやデータ(再)転送の頻度が減り、WAN遅延による影響、ネットワークエラー、パケット損失を回避します。また、ダウンロードするデータの

量を大幅に削減しますが、特別なソフトウェアのダウンロードやブラウザの設定変更は必要ありません。

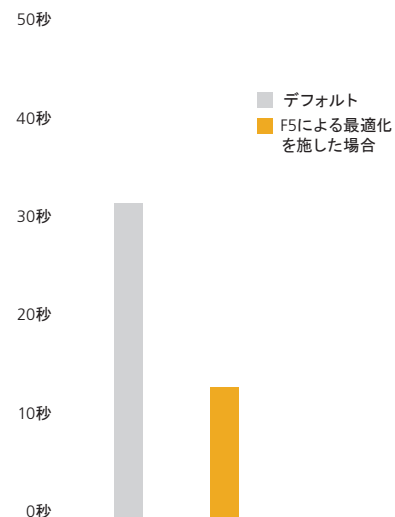
SAP製品にはビジネスクリティカルなサービスを提供する、さまざまなアプリケーション・コンポーネントが含まれています。F5を使用すると、コアアプリケーションとは関係のない処理のためにプロセッサが集中的に使用されて、これらの重要なアプリケーションが停止することはありません。一元化された高性能ネットワークデバイスが煩雑で繰り返しの多い処理（圧縮、キャッシュ、SSLなど）の負荷を軽減し、サーバの効率を大幅に向上させる包括的なソリューションを提供します。最近行われたテストでは、シナリオのひとつに500名のユーザがWANを経由してSAPアプリケーションに接続するシミュレーションが含まれていました。その結果は、F5の技術を使用した場合、SAPサーバのCPU利用率は68%から38%に削減されました。

エンドユーザのパフォーマンスを強化するため、F5では幅広い接続管理機能とTCP最適化機能を提供し、サーバのパフォーマンス向上とページのロード時間の劇的な高速化を実現しています。たとえば、数千に及ぶユーザの要求を集約してサーバ側の接続数を減らし、バックエンドシステムで要求を効率的に処理して、SAPサーバの容量を大幅に拡大します。前述の500名のユーザによるテストでも、クライアント側の1,000の接続がアプリケーション・サーバでは50に集約されています。

F5ではTCPが最適化されるため、LAN（ローカル・エリア・ネットワーク）でもWAN（ワイド・エリア・ネットワーク）でも、すべての環境でエンドユーザのパフォーマンスが向上します。高速のLANでは、F5のTCPスタックが瞬時にバッファサイズを拡張し、低遅延を検出して処理の集中化を管理します。低速のWANでは、クライアントの速度を検出し、帯域幅を見積もって、パケットの損失と修復の影響を抑制します。

F5ではユーザとSAPサーバの接続を分離して制御、個別に最適化するため、ネットワークとネットワーク上で稼働しているSAPアプリケーションに接続するすべてのデバイスで最高のパフォーマンスが確保されます。そのため、クライアントとサーバが最大公約数で通信する必要はありません。F5がクライアントの代わりに調整し、TCPの強化機能を使用するため、ネットワーク内部でサーバ用に最適化された

SAPのアプリケーション・パフォーマンス (秒数)



F5で最適化すると、低容量の回線を使用しているクライアント（遠隔地のオフィスや自宅での利用など）のダウンロード所要時間も大幅に削減されます。

接続を維持しながら、クライアント側の通信も最適化されます。たとえば、F5製品を使用したWANユーザは、Enterprise PortalやKnowledge Managementのシステムにログインした際に、パフォーマンスが2倍向上したと感じます。

また、アプリケーションのパフォーマンスを強化し、エンドユーザがSAP製品を簡単に利用できるように、SAP専用的高速化ポリシーも提供しています。SAP専用にかスタマイズされたポリシーを選択するだけで、複数の設定オプションに悩まされることなく、簡単かつ短時間で高速化します。

メリットとF5の強み

アプリケーションのセキュリティ

エンドユーザの操作性と同様に、アプリケーションのセキュリティは既存のネットワーク・セキュリティ対策に依存する企業が多いため、アプリケーションを導入しても、アプリケーションレベルのセキュリティは後回しにされるか、完全に無視される場合がほとんどです。このような誤解は多くの場合、特にSAPのようにビジネス・クリティカルなアプリケーションにおいてはコスト増大の原因になります。アプリケーションをターゲットに、通常のネットワークのセキュリティ対策では検出されない不正がますます増加しています。F5ではSAP製品と、ネットワーク上のその他のアプリケーションを保護するさまざまな対策を提供しています。

そのアプリケーション・セキュリティは他の多くのファイアウォール、侵入検知/保護システムおよびその他の署名による検証方法にはない機能を備えています。予防的なセキュリティモデルを活用し、既知のアタッキングベクトルの単純な分析やブロックではなく、既知の適切なトラフィックのみを許可します。既知のシグネチャアタックのリストに依存しているデバイスでは、アプリケーション固有の脆弱性を集中攻撃する不正ユーザを阻止できません。

F5の主なメリット

- SAP Enterprise PortalのWANユーザのログイン時間を半分以上削減します
- DSLユーザで4.5倍、高帯域幅接続で40倍、文書のダウンロードを高速化します。
- SAPサーバのCPUの使用を44%削減します。
- SAPのサーバ側の接続数を20倍削減します。
- SAPアプリケーションをWAN経由で使用した場合の帯域幅コストを大幅に削減します。

F5はパターン化されていない攻撃をリアルタイムで検出および緩和して、HTTPおよびHTTPSに対する脅威に効果的に対処できない既存のファイアウォールとIDSデバイスに高精度の保護を追加します。

攻撃がますます巧妙になり、ハッカーは、エンドポイントで正当なユーザに透過的に配布されるクッキーやその他のトークンを使用するようになっています。SAPのデフォルト設定でも、アプリケーションでユーザのハードドライブに保存されたクッキーを使用します。一般的ではないものの、不正ユーザがこのクッキーを変更して、不正にアクセスする可能性もあります。F5のデバイスはクッキーを簡単に暗号化できるため、改ざんをはじめとするクッキーを使用した攻撃を防止できます。

また、F5はインフラストラクチャやサービス、あるいはそれらに関連する脆弱性につながる手掛かりをハッカーなどに発見されないよう、すべてのアプリケーション、サーバエラーコード、URL リファレンスを仮想化して隠蔽します。さらに、OSとWebサーバを特定できる情報（バージョンストリング、メッセージ、署名および指紋など）をメッセージのヘッダから取り除き、HTTPのエラーメッセージを非表示にし、ユーザに送信するページからアプリケーションのエラーメッセージを削除すると同時に、サーバのコードや非公開のHTMLコメントが公開されたWebページに表示されていないか確認します。

F5にはネットワークやネットワーク上で稼働中のSAPアプリケーションに接続する、リモートユーザに対する詳細なエンドポイント・セキュリティ機能もあります。リモートユーザがF5デバイスにログオンしてネットワークにアクセスする前に、そのユーザのPCでアンチウイルスやファイアウォールが実行されているか確認するほか、その更新状況やOSのパッチの適用など、さまざまなログオン前チェックが実行されます。復旧ページにユーザを転送してさらに詳細な検査を行ったり、そのユーザに対してアンチウイルスまたはファイアウォールを設定できます。F5のリモートアクセス機能では、ネットワークアクセス時に使用するユーザ名とパスワードに加えて、大手ベンダーによる2要素認証もサポートしています。

また、キャッシュ・クリーンアップ機能により、リモートユーザがリモートアクセスのセッションを終了したときに、クッキー、ブラウザの履歴、オートコンプリート情報、ブラウザのキャッシュ、一

時ファイルのほか、セッション中にインストールされたすべてのActiveXコントロールがクライアントPCから削除されます。使用後に情報が一切残らないことは、キオスクなど公共のコンピュータから接続するユーザにとっては重要です。

F5が誇る高度なセキュリティ機能を備えたデバイスは、ネットワークとアプリケーションに包括的なセキュリティを提供します。SAPアプリケーションおよびそのアプリケーションに含まれる情報は完全に保護されます。

総合的なセキュリティ保護とアクセスコントロール

セキュリティの強固なインフラストラクチャを用意したら、次に、セキュリティポリシーを適用してアプリケーションへのネットワークアクセスを制御します。SAPアプリケーションを導入している企業の多くはパートナー、ベンダーおよび請負業者にもSAPとネットワークへのアクセスを提供しますが、そのアクセスは制限して慎重に管理する必要があります。アクセスの提供はユーザによってアクセスレベルが異なるだけでなく、アクセスに必要なデバイスも異なるために複雑化しがちです。F5では、エンドユーザ、クライアントタイプ、アプリケーション、アクセスネットワーク、あるいはネットワークリソースに関係なくアクセスコントロールを提供するための、完全なアプローチを提供しています。

また、ユーザグループの追加やユーザグループをベースにしたアクセスの制限も容易です。たとえば、SAPアプリケーションの一部にアクセスするビジネスパートナーで構成されるグループ、SAPの1つのアプリケーションのみにアクセスが許可された請負業者のグループなどを作成できます。アクセス制御が一元化されているため、このような制限の設定と適用も容易です。また、デバイス情報（IPアドレスや時刻など）を収集し、リソースを提供すべきかどうかを判断します。F5のソリューションはあらゆるネットワークやデバイスに対するコントロール機能を備えているため、リモートユーザ、ワイヤレスLANおよびLANに対して複数のアクセス・コントロール・ソリューションを導入する必要はありません。

また、仮想の管理ドメインをサポートしているため、単一のデバイスを複数のアプリケーション・チームで管理しても障害が発生することはありません。

メリットとF5の強み

すべてのユーザが管理ドメインに割り当てられ、割り当てられたユーザに表示されるオブジェクトが定義されます。デバイスにログオンして特定のオブジェクトのステータスとトラフィック量を確認するだけの読み取り専用ユーザ、デバイス上のすべてのオブジェクトの設定を変更できる管理ユーザなど、各ユーザには複数レベルのアクセスを定義できます。この定義によって、会議や適切な管理者の追跡に費やす時間が短縮され、アプリケーション管理者の必要に応じたアプリケーション管理能力が向上します。また、ビジネスプロセスが合理化され、運用担当者の効率も向上します。

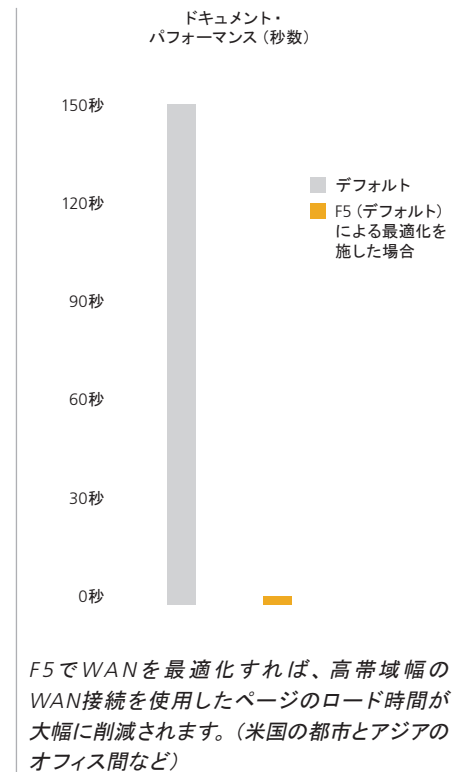
ビジネス・コンティニュイティとディザスタ・リカバリ

IT管理者はSAPのパフォーマンスとセキュリティを確保するだけでなく、予期せぬ切断やデータセンター全体が停止する最悪の事態にも備える必要があります。これは、データ保護やディザスタリカバリに関する業界や政府の新しい規制に対応する上で特に重要です。F5はビジネスクリティカルなSAPアプリケーションの可用性を常時確保できる製品として、市場でも独自の地位を確立しています。

問題が発生した場合、たとえばそれが吹雪のために社員の大半が出勤できなくなるなど、めったに発生しない問題であっても、F5はネットワーク、SAPおよびその他のアプリケーションへのリモートアクセスを優れた安全性で提供します。F5のリモートアクセス・ソリューションは導入と操作がIPSECよりも容易なだけでなく、ユーザがソフトウェアを事前にインストールや設定しなくても、ボタンをクリックするだけでSAPアプリケーションにアクセスできるように設定できます。また、TCPの圧縮とキャッシュの追加によりパフォーマンスを強化しているため、エンタープライズ・ネットワークにリモートアクセスするユーザも快適に利用できます。その証拠に、SAPではF5のリモートアクセス・ソリューションを使用しています。SAPの約7,000名の社員がF5のSSL VPNを使用して毎日アプリケーションにアクセスしています。

F5はユーザの企業が使用しているSAPだけではなく、ISPに障害が発生した場合もサポートします。マルチホーム化された導入も簡単なため、ISPのサービスや特定IPアドレスのプロック、ASN、ハイエンドルータ、ISPの障害からネットワークを保護するためのBGPの複雑な設定も不要です。F5の技術を使用して複数の小規模な接続を集約すれば、単一の高帯域幅接続に投資する必要もなくなります。そのため、企業は成長に合わせて無制限にサービスを拡大できます。F5は複数のWAN ISP接続の可用性とパフォーマンスをシームレスに監視し、サイトへの双方向トラフィックフローをインテリジェントに管理して、フォールト・トレランスを備えた最適なインターネット・アクセスを提供します。また、リンク全体でエラーを検出して、エンドツーエンドの信頼性の高いWAN接続を提供します。各接続のヘルスおよび可用性を監視し、リンクまたはISPへの障害を検出します。障害が起きた場合、ユーザが接続を続けられるように、トラフィックは他の利用可能なリンクに動的に転送されます。

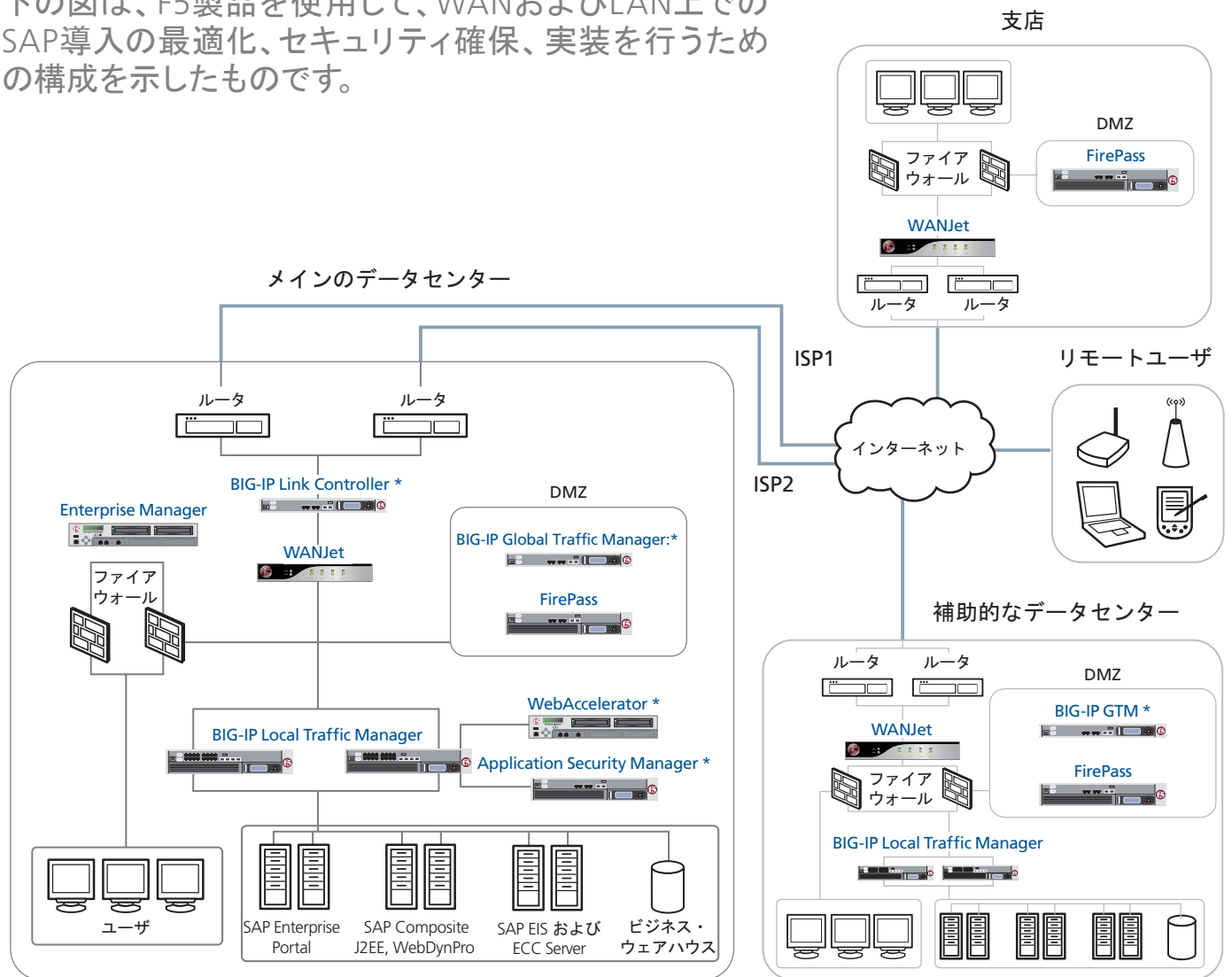
SAPアプリケーションは一般的に、企業のネットワーク・トラフィックのうち、わずかな割合を占めているに過ぎません。ただし、そのトラフィックはビジネス・コンティニュイティにとって重要です。アプリケーションは通常、24時間365日可用性が必要とされ、パフォーマンスの低下はビジネスに大きく影響します。ネットワーク・パフォーマンスのわずかな低下でさえSAPアプリケーションのユーザに影響し、アプリケーションのレスポンスが遅延するとユーザの生産性が低下します。たとえば、コールセンターの効率は処理量と顧客の待ち時間などのメトリクスで測定されますが、ネットワーク接続が遅延するとその両方に影響が及びます。ユーザがSAPアプリケーションのレスポンスを待つことになれば、電話1件当たりの処理が遅れ、1日の処理量が減少します。また、顧客サービスのコストにも悪影響を及ぼして利益が縮小します。



F5はサイトのフェイルオーバーおよびビジネス・コンティニュイティに役立つ、業界で最も包括的なソリューションを提供します。その包括的なソリューションでは、サイトのアプリケーションの可用性・チェックを総合的に実行できるだけでなく、すべてのトラフィックを動的かつ透過的にバックアップ・データセンターに移行する場合、サイト全体をフェイルオーバーする場合、または影響を受けるアプリケーションだけを制御する場合の条件も定義します。

F5およびSAPのグローバルな導入

下の図は、F5製品を使用して、WANおよびLAN上でのSAP導入の最適化、セキュリティ確保、実装を行うための構成を示したものです。



* BIG-IP LTMシステムの一部として使用できます。

SAPおよびF5のソリューション・ドキュメント

導入ガイド

[Deploying the F5 BIG-IP LTM System with SAP](#)

BIG-IP LTMシステムとSAPの設定手順をステップバイステップで詳細に説明しています。

Success Story

[SAP Success Story](#)

このF5のケーススタディでは、SAPが実施したVPN技術からF5のFirePass SSL VPNへの移行について説明しています。

F5とSAPのパートナーシップに関する詳細は、F5 Solution Centerの[SAP Partner Showcase](#)を参照してください。

F5提供製品の概要

BIG-IP LTM

BIG-IP Local Traffic Manager (LTM) は、サービス品質や管理品質を確保し、コンテンツの配信にビジネスポリシーや規定を適用します。また、増大するトラフィック・ボリュームに対応し、使用するアプリケーションを安全に配信しながら、運用効率やコスト管理を改善、今後のアプリケーションやインフラストラクチャの変更に対する柔軟性を維持して投資を保護します。

製品モジュール (以下のモジュールはスタンドアロン・アプライアンスとしても提供)

BIG-IP GTM: BIG-IP Global Traffic Manager(GTM) は、世界中に分散した複数のデータセンター間で稼動するアプリケーションに対し、高い安定性、最大のパフォーマンス、およびグローバルな管理を実現します。またFirePass VPNをシームレスに仮想化して、自動的に常時利用可能なアクセスコントロールを提供します。

BIG-IP ASM: Application Security Manager (ASM) は、特定のWebアプリケーション、あるいはWebアプリケーション全体を標的とした攻撃からアプリケーションレイヤを保護することで、アプリケーションが常に利用可能な状態で、最適なパフォーマンスを提供できるようにします。

WebAccelerator: WebAccelerator™は、一連のインテリジェント技術を備えたWebアプリケーション用のソリューションで、ユーザのパフォーマンスに影響を与えるブラウザ、Webアプリケーションのプラットフォーム、WANの遅延に伴う問題を解決するように設計されています。

BIG-IP LC: BIG-IP Link Controllerは、マルチホーミング時のインターネット回線の安定性やパフォーマンスを監視し、フォールト・トレラントで最適なインターネット・アクセスを提供しながら、サイトへの双方向トラフィックフローをインテリジェントに管理します。

機能モジュール: 機能モジュールは、BIG-IPトラフィック管理プラットフォームに追加できる個々の機能パックです。機能モジュールには、メッセージ・セキュリティ、インテリジェント圧縮、L7レートシェイピング、IPv6ゲートウェイ、アドバンスクライアント認証、SSLアクセラレーション、Fastキャッシュ、およびアドバンス・ルーティング・モジュールが含まれています。

FirePass

F5のFirePass® SSL VPNアプライアンスは、Webブラウザを使用する社内アプリケーションとデータに、安全なアクセスを提供します。卓越したパフォーマンスとスケーラビリティに加えて、使いやすさ、エンドポイント・セキュリティを併せ持つFirePassを使用することで、社内でも外出先でも、企業データの安全性を確保しながら、高い生産性をもたらします。

WANJet

WANJet®は、WANを利用するすべてのアプリケーションにLANと同等レベルのパフォーマンスを実現する、アプライアンス・ベースのソリューションです。WANJetは、ファイル転送、電子メール、クライアントサーバ・アプリケーション、データのレプリケーションなどを加速し、すべてのWANユーザに快適な高速パフォーマンスを提供します。

Enterprise Manager

F5が提供するアプライアンスベースのEnterprise Managerによって、ネットワーク内に存在するすべてのF5製品の検出および管理を一元化します。Enterprise Managerを使用すると、ディザスタ・リカバリ・プランニング用にデバイスの設定をアーカイブ保存/保護できます。また、新しいデバイスの設定を中央集中で行うため、各デバイスを手動で操作する必要がなく、ソフトウェア・アップグレードやセキュリティパッチなどを、容易にそして短時間で実行します。

iControl API

iControlはF5が各BIG-IP LTMシステム上で展開しているSOAP APIです。iControlは、アプリケーションとネットワーク間に自動化機能を提供し、その優れた性能と柔軟性により、アプリケーションとネットワークの両方で信頼性、セキュリティおよびパフォーマンスが向上します。また、F5の開発者向けコミュニティ・サイトであるDevCentralには、iControlアプリケーションとコードのサンプルが掲載されています。

