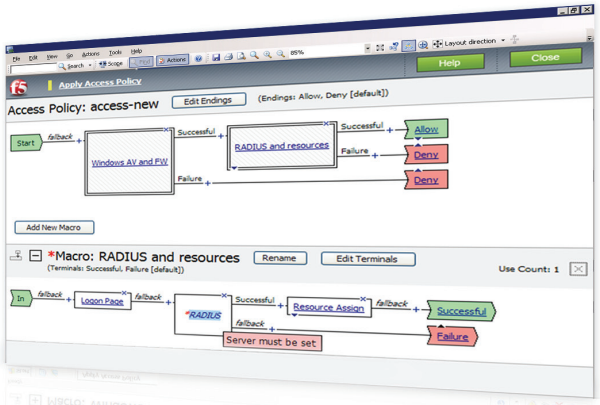
BIG-IP Access Policy Manager

データシート

目次



コスト効率に優れた統合アクセス制御および拡張の実現

今日、アプリケーションやデータなどのビジネスリソースは従来のビジネスの境界の内外両方からアクセスされます。ローカルやリモートの従業員、パートナー、および顧客が、コンテキストがなくセキュリティが確保されていない状態でアプリケーションにアクセスすることも珍しくありません。ポリシーの集中型制御ポイントはコンテキストに基づくアクセスを提供します。安全で拡張性に優れたダイナミックな環境を管理するためにも欠かせません。

BIG-IP® Access Policy Manager™ (APM) は柔軟で高パフォーマンスのアクセスおよびセキュリティ・ソリューションであり、アプリケーションおよびネットワークへの統合グローバルアクセスを提供します。リモートアクセス、LAN アクセス、ワイヤレス接続を単一の管理インターフェイスに収束および統合し、管理しやすいアクセスポリシーを提供することによって、BIG-IP APM は貴重な IT リソースを節約し、コスト効率に優れた拡張を可能にします。

主な特長

統合グローバルアクセス
リモートアクセス、内部 LAN アクセス、ワイヤレスアクセスを1つのインターフェイスに統合します。

統合および簡素化
Web アクセスプロキシ層の代わりとして機能し、OAM、XenApp、および Exchange と連携して、インフラストラクチャや管理のコストを削減します。

集中型アクセス制御
簡素化された一元的な制御ポイントで、コンテキストを認識するポリシーをダイナミックに適用して、アプリケーションと Web サイトへのアクセスを管理します。

優れたアクセスとセキュリティを保証
包括的なエンドポイント・セキュリティによって、データ損失、ウイルス感染、デバイスへの不正アクセスから組織を保護します。

安全な Web アクセス
不適切な Web サイトや危険性のある Web サイト、マルウェアに感染した Web アプリケーションへのユーザアクセスを制御し、高度な web の脅威から保護します。

柔軟性と拡張性の確保
すべてのユーザを簡単に、迅速かつコスト効率よくサポートします。

ICSA labs CERTIFIED SSL VPN

ICSA labs CERTIFIED FIREWALL - CORPORATE

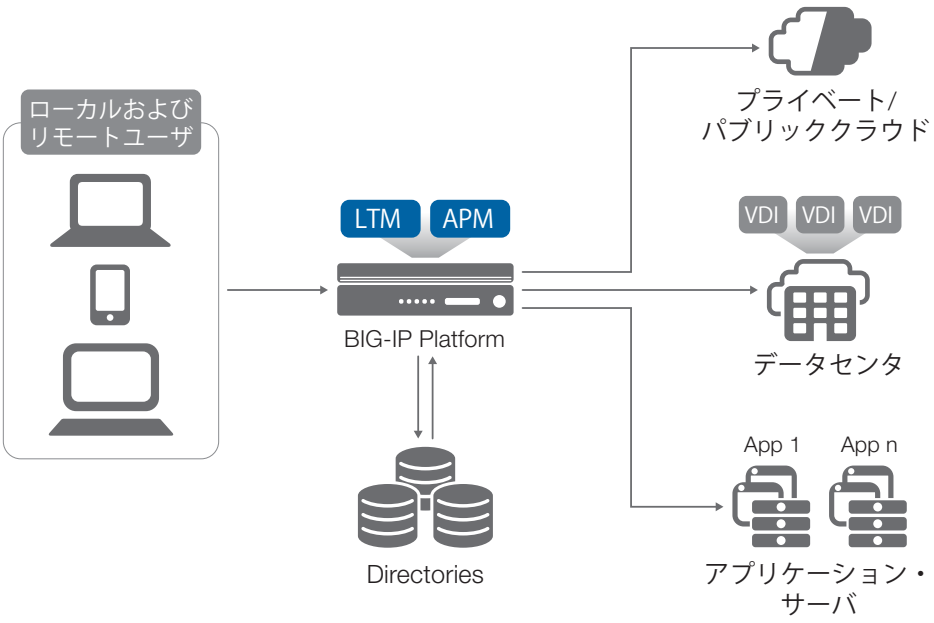
統合グローバルアクセス

モバイルワーカーの増加に伴い、企業リソースにアクセスするネットワークやデバイスの種類が多様化しています。その結果、リモートユーザに安全で高速なアプリケーション・パフォーマンスを保証することが大きな課題となっています。

すべてのアクセスに対応する単一ソリューション

BIG-IP APM はアプリケーションとユーザの間に配置され、ネットワーク上の戦略的コントロールポイントとして機能します。アクセス用のインフラを統合し、外部ユーザに対してコンテキストを認識するポリシーベースのアクセス制御を実施することで、公開されているアプリケーションを保護します。また、すべてのネットワークおよびデバイスから企業リソースへの安全なリモートアクセスも提供します。

リモートアクセス、LAN アクセス、ワイヤレス接続を単一の管理インターフェイスに収束および統合し、管理しやすいアクセスポリシーを提供することによって、IT 担当者はアプリケーション・アクセスの制御に集中することができます。



BIG-IP APM は、ネットワークおよびアプリケーションへのすべてのアクセスを統合して管理します。

「常時接続」リモートアクセス

BIG-IP APM はオプションのクライアントと連携して安全なリモートアクセスを提供します。この最新の統合型クライアント BIG-IP® Edge Client® はロケーション認識とゾーン決定によって、他に類を見ない安全なポリシーベースの永続的アクセスを提供します。ユーザが家で無線ネットワークを使用していても、通勤中にモバイルカードを使用していても、社内で無線接続のプレゼンテーションを行っていても、カフェでゲストアクセス用無線を使用していても、または社内 LAN に接続していても、BIG-IP Edge Client はユーザの生産性を継続的に保証します。BIG-IP Edge Client では、VPN 接続が切断された後でも自動的にドメインを検出して接続したり、LAN 接続が検出された場合には VPN を切断することができます。

BIG-IP APM は、管理されたアクセスをリモートユーザおよびモバイルユーザに拡張し、多種多様なモバイルデバイスをサポートします。BIG-IP® Edge Portal™アプリケーション

はすべての Apple iOS、Google および Android デバイスで利用可能で、企業の Web アプリケーションへの安全なリモートアクセスを可能にします。BIG-IP Edge Client は Apple Mac、iPhone、iPad、Microsoft Windows デバイス、Linux プラットフォームで利用可能で、SSL VPN に完全に対応しています。

IPv6 ネットワークに接続を拡張

インターネットは IPv4 から IPv6 に進化しています。ビジネスの継続性を確保し、将来の拡張に対応するには、IPv4 と IPv6 の併用をサポートできるネットワークが必要となります。BIG-IP APM は IPv6 に完全に対応。真のグローバルアクセスを実現します。

統合されたインフラストラクチャと簡素化された管理

企業全体のコスト効果の高いアプリケーション・アクセス管理と、集中型アプリケーション配信を直接 BIG-IP LTM に統合することにより、BIG-IP APM ではアプリケーションの認証、許可、アカウント（AAA）サービスの導入が大幅に簡素化されます。

シングルサインオン

BIG-IP APM は、複数のドメイン間のシングルサインオン（SSO）と Kerberos のチケット処理をサポートしています。そのため、すべてのアプリケーションで、米国政府で採用されている CAC カードや Active Directory 認証などの認証方式を使用できます。ユーザは Kerberos レルムの一部であるバックエンド・アプリケーションおよびサービスに自動的にサインオンします。このため、サポートされている認証方式のいずれかでエンドユーザが 1回認証されると、ユーザに対して透過的に、ユーザ認証が実行されるようになります。

Security Assertion Markup Language（SAML）2.0 によってアイデンティティ・プロバイダ（IdP）が開始する接続とサービスプロバイダ（SP）が開始する接続を両方ともサポートし、BIG-IP の SSO はさらに拡張されます。SSO が企業データセンタの外部のクラウドベース・アプリケーションにも拡張され、企業の BIG-IP プラットフォーム全体の ID フェデレーションが可能になります。その結果、SSO で複数のアプリケーションにログインするための時間を最小化し、クラウド、Web、仮想デスクトップ装置（VDI）、クライアント / サーバアプリケーションに対する統合ユーザポータルを実現できます。

Exchange サービスの自動同期

BIG-IP APM は、Apple iPhone などの Microsoft ActiveSync プロトコルを使用するモバイルデバイス上での Microsoft Exchange との E メール、カレンダー、連絡先の同期をサポートしています。Microsoft Outlook Web Access、ActiveSync、Outlook Anywhere の接続を許可するための認証ゲートウェイを追加する必要がなくなり、インフラの統合を推進してユーザの生産性を向上させることができます。Exchange 2010 に移行すると、BIG-IP APM は Active Directory と連携して、長期間にわたるメールボックスのシームレスな移行を可能にします。移行の完了後、BIG-IP APM はユーザ、デバイス、ネットワークの種類を問わず、単一の URL アクセスで Exchange への管理されたアクセスを提供します。

統合 AAA インフラストラクチャ

他の認証ソリューションでは、アプリケーションのコーディング、別個の Web サーバエージェント、または個別のプロキシを使用するため、管理や費用、拡張性に関して大きな問題が生じることがあります。BIG-IP APM では、BIG-IP 上で直接 AAA 制御を行うため、多くのアプリケーションに共通のアクセスポリシーを適用し、承認の状態を一元的に把握できます。AAA インフラストラクチャを統合し、冗長層を削除して管理を簡素化し、設備投資や運用コストを削減できます。

Oracle 向けの統合アクセス

BIG-IP APM と Oracle Access Manager の統合により、Oracle アプリケーション向けのアクセスポリシーを1か所で設計し、ポリシーベースのアクセスサービスを管理することができます。プラグインと Web 認証プロキシの統合は、設備投資や運用コストの削減に貢献します。

仮想化アプリケーション環境のアクセスの簡素化

BIG-IP APM を使用すると、仮想化ソリューションのアプリケーション·デリバリ·コンポーネントやセキュリティ・コンポーネントをダイナミックに制御して、アクセス、セキュリティおよびポリシーの管理を統合することができます。たとえば、一般的な Citrix XenApp/XenDesktop の実装では、管理者は Citrix 認証管理、Secure Ticket Authority (STA)、NetScaler、および XenApp Services サイト (Citrix ソースのエンタープライズ· デプロイが必要) を BIG-IP APM に置き換えることができます。

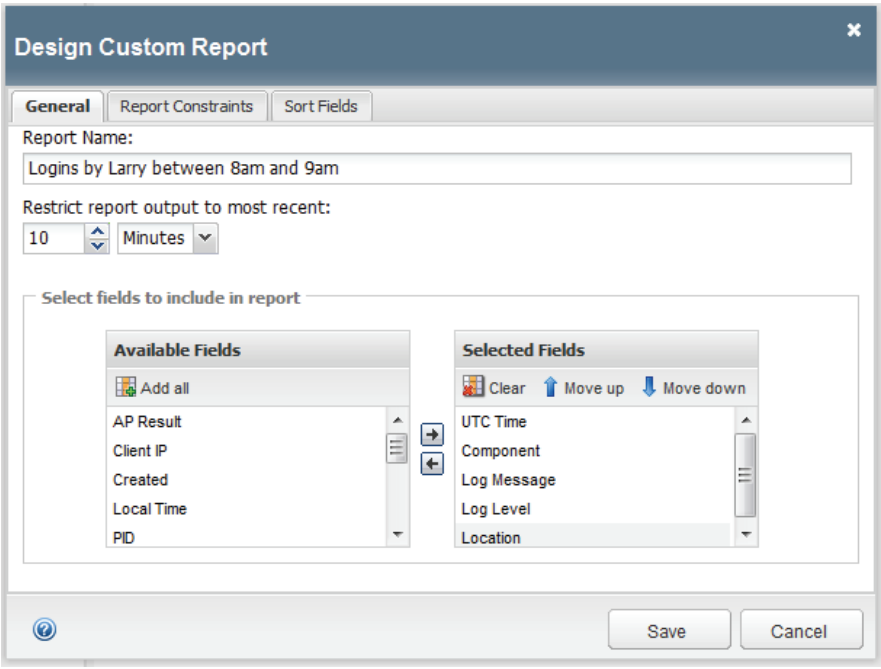
BIG-IP APM は、VMware View および Citrix XenApp/XenDesktop の同時使用をサポートしており、他の技術を混在させることもできます。さらに、BIG-IP APM は、単一の拡張可能なアクセス制御ソリューションを提供します。リモートおよび LAN 両方のアクセスポリシーを含んでおり、バックエンドサーバの設定を変更する必要もありません。このソリューションを他のアプリケーションに拡張して、シンプルで拡張性に優れた低コストのエンタープイライズ· インフラストラクチャを提供することもできます。

先進的レポート

ログやイベントの詳細な表示で、アクセスポリシー・セッションを詳細に把握できます。技術提携パートナーである Splunk のレポートを利用すれば、BIG-IP APM で Web アクセスおよびトラフィックの傾向を観察し、長期的な調査のためデータをアグリゲートして、問題への対応スピードを上げ、予期しない問題をユーザが気付く前に特定することができます。Splunk は、大規模で高速な分析・検索ソリューションです。

BIG-IP APM ではレポートをカスタマイズして、情報分析のための詳細なデータと統計を得ることができます。たとえば、以下の項目を含む詳細なセッションレポートを作成できます。

- アクセスエラー数
- ユーザ数
- アクセスされたリソース
- グループの使用状況
- IP 地理位置情報



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。

すぐ使用できる設定ウィザード

BIG-IP Access Policy Manager を使用すると、統合サービスおよび承認サービスの迅速な設定と導入が容易になるため、管理コストが削減されます。設定ウィザードには、構築済みのアプリケーション·アクセス·ウィザードやローカルトラフィック仮想デバイスウィザードが含まれています。これによりオブジェクトの基本セットと一般的導入向けのアクセスポリシーが作成され、必要なオブジェクト設定をサポートする詳細設定も自動的に作成されます。ステップバイステップの設定、コンテキスト依存のヘルプ、レビュー、サマリにより、BIG-IP APM では認証および承認の設定を簡単かつ迅速に行うことができます。

リアルタイムのヘルスデータへのアクセス

BIG-IP にあるアクセスポリシー・ダッシュボードでは、アクセスの状態の概要を一目で把握することができます。アクティブセッションやネットワークアクセスのスループット、新しいセッション、およびネットワークアクセス接続をデフォルトのテンプレートで表示したり、ダッシュボード・ウィンドウの選択肢からカスタマイズした表示を作成できます。必要な統計をウィンドウペインにドラッグアンドドロップすれば、アクセスの状態をリアルタイムで知ることができます。

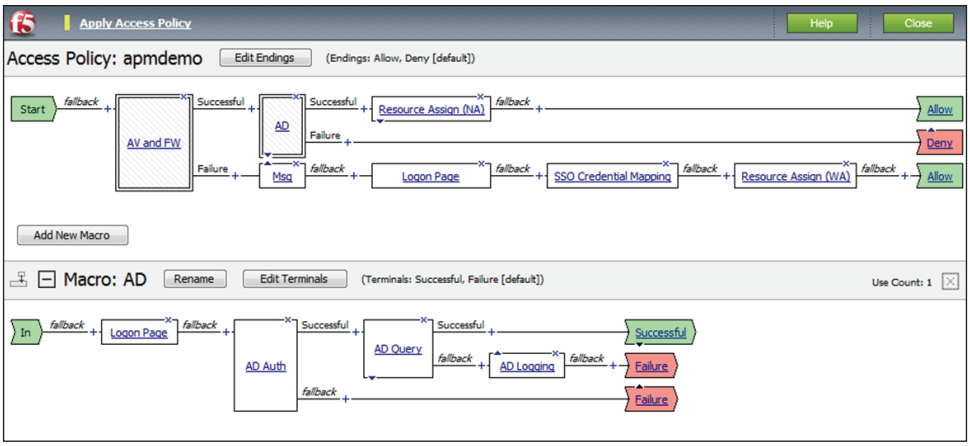
ダイナミックな集中型アクセス制御

コンテキストを認識し、ポリシーベースでアクセスを決定することで、BIG-IP APM は企業のセキュリティ標準へのコンプライアンスを強化し、ユーザが適切なアプリケーション·アクセスを利用しながら生産性を維持できるようにします。

先進的なビジュアル・ポリシー・エディタ

先進的な GUI ベースのビジュアル・ポリシー・エディタ（VPE）で、詳細なアクセス制御ポリシーを個々に、あるいはグループごとに、簡単に設定して管理することができます。

数回クリックするだけで、ダイナミックなアクセスポリシーを迅速かつ効率的に作成したり編集することができます。たとえば、RADIUS に統合された認証サーバポリシーを設計したり、アクセスが承認された後リソースを割り当てたり、ポリシーに準拠していないアクセスを拒否できます。地理位置情報エージェントは、自動ルックアップおよびロギング機能を提供します。これらの機能によって設定プロセスが簡素化され、ユーザアクセスルールを組織の地理位置情報ポリシーに従ってカスタマイズすることができます。ポリシー制御を一元化することで、VPE はアクセス管理のコスト効率を高めます。



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。

ダイナミックなアクセス制御

BIG-IP APM はアクセス制御リスト（ACL）を使用してアクセス認証を行い、レイヤ 4 ACL とレイヤ 7 ACL をダイナミックに適用してセッションごとにユーザを承認します。レイヤ 4 ACL とレイヤ 7 ACL はどちらもポリシー施行ポイントとしてエンドポイント条件に基づいてサポートされます。BIG-IP APM では、セッションごとのダイナミックなレイヤ 7（HTTP）ACL を使用して、認証された個々のアプリケーションおよびネットワークに、個別またはグループごとのアクセスを承認できます。ACL は、ビジュアル･ポリシー･エディタで簡単に作成できます。

アクセスポリシー

BIG-IP APM で認証および承認用のアクセスポリシーを設計し、オプションでエンドポイント・セキュリティのチェックを行い、企業ポリシーへのユーザのコンプライアンスを強化することができます。あらゆるデバイスからのすべての接続に対してアクセスプロファイルをまとめて 1 つ定義したり、さまざまなアクセス方法に対して複数のプロファイルを作成し、それぞれに独自のアクセスポリシーを設定することができます。たとえば、アプリケーション・アクセス認証用、ダイナミック ACL 接続用のポリシーを作成できます。ポリシーを設定すると、ネットワークはコンテキストを認識するようになり、ユーザがだれであるか、ユーザがいつ、どのようにアプリケーションにアクセスしようとしているか、ユーザがどこからアプリケーションにアクセスしようとしているか、また現在のネットワークがどのような状態であるかを、アクセス時に理解します。

コンテキストベースの承認

BIG-IP APM ではアイデンティティをネットワークに導入することによって、ユーザアクセスに対するシンプルな集中型の制御が可能になります。何万ものユーザが 1 つのアプリケーションにアクセスする場合、BIG-IP APM では SSL 暗号化処理の負荷を軽減し、認証お

よび承認サービスを提供します。またオプションでアプリケーション・サーバに対する単一の安全な SSL 接続を確立します。コンテキストベースの認証により、ユーザのナビゲーションを完全かつ安全に制御できます。

優れたセキュリティ

コンテキストを認識し、ポリシーベースでアクセスを決定することで、BIG-IP APM は企業のセキュリティ標準へのコンプライアンスを強化し、ユーザが適切な Web アクセスを利用しながら生産性を維持できるようにします。

VPN テクノロジ

BIG-IP APM はオプションのクライアントと連携して、モバイルワーカーやリモートワーカーに SSL VPN リモートアクセスを提供します。リモート接続用の Datagram Transport Layer Security (DTLS) モードは、遅延が許容されないアプリケーションの保護およびトンネリングに最適です。ブランチオフィスとデータセンタ間のトラフィックに対しては、IPsec 暗号化が有効です。F5 の統合アクセス・ソリューションを使用すると、世界各地に点在するインフラストラクチャ全体に対してエンドツーエンドのセキュリティを確保することができます。

VMware View ネイティブプロキシ対応 (PCoIP)

最新の APM ではネイティブで VMware View 向けのプロキシ機能を実装しました。これにより、当該 VMware View 環境においては APM の利便性が大幅に向上し、今まで以上の快適な VDI 環境を実現します。トンネルを張る必要が無くなることによる管理性の向上、クライアントソフトのインストールが不要になる、などのメリットがあります。

強力なエンドポイント・セキュリティ

BIG-IP APM はブラウザベースのインスペクション・エンジンを使用して、デバイスのセキュリティを調査し、そのデバイスが企業ドメインに属しているかどうかを判定します。その結果を基にダイナミックアクセス制御リストを割り当てて、コンテキストベースのセキュリティを提供します。デバイスの MAC アドレス、CPU ID、HDD ID に加え、Apple iOS または Google Android を実行しているモバイルデバイスの場合、エンドポイント検査ではモバイルデバイス UDID とモバイルデバイスがジェイルブレイクされたり、root 化されていないかをチェックします。ハードウェアの属性をユーザロールにマップして、アクセス制御用の決定点を複数設定できます。ユーザセッションの終了時に、ブラウザ・キャッシュ・クリーナーがすべての機密データを自動的に削除します。

ダイナミック・ウェブトップ

ダイナミック・ウェブトップには、認証後にユーザが利用できる Web ベース・アプリケーションのリストが表示されます。ウェブトップのコンテンツ表示は、ユーザが表示を承認されたリソースに限定されるという点でダイナミックであるといえます。ウェブトップは、ユーザ ID、コンテキスト、およびグループメンバシップに基づいてカスタマイズできます。SAML 対応の SSO でセットアップし、ユーザは透過的に利用することができます。

アプリケーション・トンネル

エンドポイントがセキュリティ・ポリシーに準拠していない場合、アプリケーション・トンネルが特定のアプリケーションへのアクセスを提供します。ネットワーク・アクセス・トンネルをフルオープンしないため、セキュリティのリスクが低減されます。たとえば、モバイルユーザは Microsoft Outlook クライアントをクリックするだけで、どこからでも E メールに安全にアクセスできます。アプリケーション・トンネルは WAN 向けに完全に最適化されているため、アダプティブ圧縮、高速化、および TCP 最適化技術を活用したアプリケーション接続で、コンテンツを効率的にユーザに配信できます。

保護されたワークスペースの暗号化された環境

BIG-IP APM は高度な暗号を使用して、安全なローカル・コンピューティング環境を必要とするユーザに保護されたワークスペースを提供します。このモードでは、ユーザは保護されたワークスペース以外の場所にファイルを書き込むことができません。一時フォルダのコンテンツやブラウザキャッシュはセッションの終了時に削除されるため、データが最大限保護されます。Microsoft Windows 8、Windows 7（32 ビット）、WindowsXP、WindowsVista のユーザを保護されたワークスペースに自動的に切り替えるように、BIG-IP APM で設定することができます。

Java パッチによる安全なアクセス

一般的に、ユーザが IBM 端末エミュレータなどの Java アプレットを開くと、任意のポートでネットワーク接続が開きますが、ファイアウォールによってブロックされることがあり、その場合は SSL によってトラフィックが保護されます。その結果、リモートユーザはアプレットを使用できません。BIG-IP APM は Java をリライトしてサーバ Java アプレットをリアルタイムで変換（パッチ）し、そのアプレットを実行するクライアントが、認証済みの BIG-IP APM セッションで SSL を使用して BIG-IP APM から接続できるようにします。BIG-IP APM では、1 回リライトが行われるとパッチ済みの Java が RAM キャッシュに格納されるため、毎回リライトを実行する必要はありません。

包括的なアプリケーション・アクセスとびセキュリティ

効果的なマルチソリューション BIG-IP プラットフォームにより、アクセスのパフォーマンスを低下させることなくアプリケーション・セキュリティを強化できます。BIG-IP APM および BIG-IP® Application Security Manager™（ASM）は BIG-IP Local Traffic Manager アプライアンス上で一緒に稼働し、攻撃からアプライアンスを保護するとともに、階層化されたきめ細かいアクセス制御を柔軟に提供します。攻撃はすぐにフィルタリングされるため、アプリケーションの可用性とセキュリティが保証され、ユーザのアクセスが最適化されます。この統合ソリューションを使用すれば、PCI DSS などの地域の規制への準拠を徹底できるため、違反金の支払いを最低限にし、企業のデータ損失を防ぐことができます。またネットワークに新しいアプライアンスを導入する必要がないオールインワンのソリューションで、費用の削減が可能です。

Secure Web Gatewayサービス

会社支給や個人のコンピュータやモバイルデバイスを使用して、オンサイトやリモートで会社の業務を行っている場合は、権限のあるユーザによるインターネットの利用に関する企業のコンプライアンスポリシーを確実に実施することが重要です。これは、F5® Secure Web Gateway サービスによって実現できます。

Secure Web Gatewayには、URLフィルタリングサービスとSecure Web Gatewayサービスというオプションがあります。いずれも 1 年または 3 年のサブスクリプションで利用できます。F5 からの URL フィルタリングサービスは、対象とする URL に関連づけられたカテゴリとリスクに基づいて Web サイトまたは Web アプリケーションへのアクセスを制御します。Secure Web Gateway サービスには URL フィルタリング機能が含まれていますが、リターン HTTP/HTTPS トラフィックをスキャンして、公開されている Web ページ内でホストされているマルウェアや悪意あるスクリプトもブロックします。

URLフィルタリング

URL フィルタリングを使用すると、業界や政府の規制や企業で受け入れ可能なインターネットの利用に関するポリシーへの準拠を確実に行うことができます。Secure Web Gateway サービスの URL フィルタリングは、Web サイトや数百もの Web ベースのアプリケーション、

プロトコル、ビデオへのアクセスを制御します。URL フィルタリングはカスタマイズ可能で、企業が Web ベースの脅威やデータの漏洩にさらされる危険を低減できます。

URLカテゴリ化データベース

Secure Web Gateway サービスは、パワフルな URL カテゴリ化エンジンとデータベースを使用して、インターネットと Web 全体で 4,000 万以上の URL を常に分類しています。URL カテゴリ化は、既知の Web ページに対してリアルタイムで分類情報を適用し、新しい Web ページや URL を評価します。高度な機械学習を使用してコンテンツに基づき Web ページをすばやく評価するため、フォールスポジティブが最小限に抑えられ、URL 分類が改善されます。URL カテゴリ化はコンテキストを認識し、20 以上の特性を使用して、Web ページと URL レピュレーションを評価、判断します。

Webセキュリティ

Secure Web Gateway サービスはリターン HTTP/HTTPS トラフィックをスキャンして、Web ページ内のマルウェアや悪意あるスクリプトも検出してブロックします。これは、10,000 以上の Web のマルウェア分析が含まれる堅牢なマルウェアデータベース、さらに、一般的な脅威や特殊な脅威を識別して除去する高度なシグネチャとヒューリスティック検出エンジンの集合を使用して実現されています。Secure Web Gateway サービスには、パワフルな分析が組み込まれており、組み合わせて使用すると、コンテンツベースでコンテキストに基づく評価を実行して、アドバンスド・パーシスタント・スレット（APT）をより効果的に検出できます。Web ページからコンテンツベースでコンテキストに基づいて収集したデータを使用し、Web のマルウェア分析からの情報と組み合わせて十分な情報を得た上での決定が可能になり、APT や他のスタンドアロンの分析で見逃される可能性のある他の複雑な攻撃の存在を示すパターンも検出できます。

リアルタイムのスレット・インテリジェンス

Web やソーシャル・メディア・コンテンツ内で脅威を検出するクラウドベースのスレッド・インテリジェンス・インフラストラクチャは、Secure Web Gateway サービスに常に最新のセキュリティデータを提供します。Web ページ、文書、実行ファイル、モバイル・アプリケーションなど、あらゆる Web、ソーシャル・メディア・コンテンツを分類し、毎日 50 億件ものコンテンツ要求を分析して、処理します。

このデータから選択した情報を使用して、複雑なオンラインの脅威の傾向を識別して、探し当てます。Secure Web Gateway サービスは、人気のある Web サイトがハイジャックされていないかを評価し、ウイルスに感染したサイトやコンテンツを監視し、ニュースやソーシャルメディアのトピックを使用して、人気のある Web サイト、ウイルスに感染したサイト、コンテンツの中で評価対象とすべきものをより多く見いだします。ビッグデータの分析、モバイル・アプリケーションのアクセス許可とプロファイル、クラウドのサンドボックスデータを活用して、新たに急速に出現するオンラインの脅威を予測して、識別します。Secure Web Gateway サービスは、ユーザが設定可能なスケジュールに基づいて、クラウドベースのスレット・インテリジェンスと同期します。

ユーザの識別

Secure Web Gateway サービスは、ユーザ・アイデンティティをネットワークアドレスまでマッピングして追跡し、透過的なユーザベースのセキュリティポリシーを F5 User Identity Agent 経由で実行できます。F5 User Identity Agent は Windows ベースのサーバで実行され、Active Directory ドメインコントローラから情報を取得します。F5 User Identity Agent を使用すると、Secure Web Gateway サービスでユーザ・アイデンティティごとのアクティビティを完全に追跡できます。

グラフィカル・セキュリティ・レポートと包括的なログ

システム管理者は Secure Web Gateway サービス内の GUI を使用して、さまざまなセキュリティ分析レポートを表示、エクスポートできます。これらのレポートによって、管理者は発信および受信 Web トラフィック、インターネットの利用、ポリシー実行を完全に可視化できます。Secure Web Gateway サービスは、ユーザのインターネット・アクティビティをタイムスタンプ、送信元 / 宛先 IP アドレス、ユーザ名、URL、ブロックステータスなどのフォレンジックの詳細とともにログに記録します。ログは F5 のログパブリッシャー経由で ArcSight や Splunk などのよく知られたセキュリティ情報およびイベント管理（SIEM）ソリューションに公開できます。

柔軟な導入オプション

Secure Web Gateway サービスは、明示的プロキシを使用して、1 つのスイッチポート接続を使用したネットワークの任意の場所にインストールした Secure Web Gateway サービスを実行する BIG-IP APM で柔軟に導入でき、中断やネットワーク配線の変更は必要ありません。Secure Web Gateway サービスは、インラインの透過的プロキシで、すべての HTTP および HTTPS トラフィックを透過的にインターセプトするように設定された転送プロキシを使用して導入することもでき、ネットワーク設定変更の必要性が軽減されます。

柔軟性、高パフォーマンス、および拡張性

BIG-IP APM は高速アプリケーション・アクセスと高いパフォーマンスを実現します。ユーザは生産性を維持し、企業は迅速かつコスト効率に優れた拡張を行うことができます。

柔軟な導入

BIG-IP APM は、多様なアクセスのニーズに対応する 3 つの方法で導入することができます。BIG-IP LTM のアドオンモジュールとして導入すると、公開アプリケーションを保護できます。BIG-IP Edge Gateway と使用すると、リモートアクセスを高速化することができます。また、BIG-IP LTM Virtual Edition 上で使用すると、仮想化環境でアプリケーション・アクセスを柔軟に提供できます。

仮想デスクトップのホスト

仮想デスクトップの導入では、何千ものユーザ数や 1 秒あたりの数百件の接続に対応できる必要があります。BIG-IP APM は、Microsoft Remote Desktop Protocol（RDP）のネイティブサポート、Citrix XenApp および XenDesktop の Web プロキシサポート、VMware View のフル・ネットワーク・アクセス機能を搭載しています。また、BIG-IP APM は、Java RDP クライアントとしてブラウザ上で動作する Java ベースのアプレットをクライアントに渡します。この Java RDP クライアントは、要件が記述されている場合に仮想デスクトップ装置（VDI）となる、Mac ユーザや Linux ユーザ向けの安全なリモート・アクセス・ソリューションです。拡張性とパフォーマンスに優れた BIG-IP APM のアプリケーション・デリバリ機能は、ホストされた仮想デスクトップ環境でユーザのアクセスおよび管理を簡素化します。

AAA サーバの高可用性

BIG-IP APM では、異機種混在環境で可用性の高い Web アプリケーションへのシームレスなユーザアクセスが実現するため、ビジネスの継続性が向上し、企業収益の損失につながるユーザの生産性低下を防ぎます。BIG-IP APM は、Active Directory、LDAP、RADIUS、Native RSA SecurID などの AAA サーバと統合され、BIG-IP LTM のインテリジェントなトラフィック管理機能を通じて高い可用性を提供します。

クレデンシャル情報のキャッシング

BIG-IP APM は、シングルサインオン（SSO）を実現するクレデンシャル情報キャッシングおよびプロキシサービスを提供しています。承認済みのサイトやアプリケーションにアクセスするためにユーザが複数回サインインする必要はありません。ユーザが移動すると、SSO のクレデンシャル情報が Web アプリケーションに伝送されます。サインインに要するユーザの時間を節約して生産性を向上させます。

前例のないパフォーマンスと拡張性

BIG-IP APM アクセスでは、ネットワークスピードでの SSL を提供し、1 秒あたり最大 1,600 回のログインをサポートします。Web アプリケーション・ユーザの増加が続く企業では、BIG-IP APM は迅速かつコスト効果的に拡張でき、VIPRION シャーシ・プラットフォーム 1 台あたり最大 10 万の同時接続ユーザ、または単一のハイエンド・アプライアンスにつき最大 4 万の同時接続ユーザを効率的にサポートします。

仮想クラスタ・マルチプロセッシング

BIG-IP APM は、シャーシ・プラットフォーム、BIG-IP 5200v、7200v、10200v アプライアンスでも使用可能で、仮想クラスタ・マルチプロセッシング（vCMP®）環境をサポートしています。 vCMP ハイパーバイザによって、BIG-IP APM のインスタンスを複数実行することができます。この方法では、マルチテナント用の効率的なパーティションが可能になります。ネットワーク管理者は、vCMP で高レベルの冗長性と制御を確保しつつ、仮想化を実現できます。

BIG-IP APM アーキテクチャ

BIG-IP APM は、BIG-IP Local Traffic Manager 上で稼働するモジュールとして、F5 独自の、専用 TMOS® オペレーティング・システムを使用します。TMOS はインテリジェントでモジュール式の高パフォーマンス・オペレーティング・システムであり、これにより洞察が可能になり、柔軟性や制御が備わるため、Web アプリケーションを保護できます。

TMOS は以下の機能を提供します。

- SSL 負荷軽減
- キャッシング
- 圧縮
- TCP/IP 最適化
- 先進的レートシェーピングおよび高度なサービス品質
- IPv6 Gateway ™
- IP/ ポートフィルタリング
- iRules® スクリプト言語
- 内蔵スイッチによる VLAN サポート
- リソースのプロビジョニング
- ルートドメイン（仮想化）
- リモート認証
- レポートスケジューリング
- フルプロキシ
- 鍵管理およびフェイルオーバ処理
- SSL ターミネーションと Web サーバへの再暗号化
- VLAN セグメンテーション
- DoS 保護
- システムレベルのセキュリティ保護
- BIG-IP APM および BIG-IP Application Security
- Manager の階層化
- BIG-IP APM および BIG-IP WebAccelerator の階層化
- F5 Enterprise Manager のサポート

BIG-IP APM には次のような機能があります。

- ポータルアクセス、アプリトンネル、およびネットワークアクセス
- IPv6 ready
- 詳細なアクセスポリシー施行
- 地理位置情報エージェントを含む、先進的なビジュアル・ポリシー・エディタ
- AAA サーバ認証および高いアベイラビリティ
- アプリケーション・デリバリおよび保護のための DTLS モード
- クライアント側 NTLM を含む、Microsoft ActiveSync および Outlook Anywhere のサポート
- Citrix XenApp および XenDesktop のアクセス管理の簡素化
- Microsoft RDP クライアントと Java RDP クライアントのネイティブ・サポート
- Microsoft Exchange メールボックスのシームレスな移行
- L7 アクセス制御リスト（ACL）
- プロテクテッド・ワークスペースのサポートと暗号化
- ビジュアル・ポリシー・エディタでの IP 地理位置情報
- エージェント
- シングルサインオン用のクレデンシャル情報のキャッシングとプロキシ
- 安全なアクセスのための Java パッチ（リライト）
- 仮想 VMware 環境における柔軟な導入
- Oracle Access Manager との統合
- Kerberos、クレデンシャル情報キャッシング、および SAML 2.0
- ダイナミック L4/L7 ACL によるコンテキストベースの承認
- Windows マシン証明書サポート
- Windows Credential Manager の統合
- 外部ログオンページサポート
- BIG-IP Local Traffic Manager（LTM）バーチャルサーバへのアクセス制御のサポート
- すぐに使用できる設定ウィザード
- 同時接続ユーザ数 10 万まで拡張
- ポリシールーティング
- アクセスポリシーのエクスポートおよびインポート
- 設定可能なタイムアウト
- RADIUS アカウント向けヘルスチェックモニタ
- クラスタ・マルチプロセッシング
- ランディング URI 変数のサポート
- DNS キャッシュ / プロキシサポート
- オプションのクライアントを使用する SSL VPN リモートアクセス
- BIG-IP Edge Client による常時接続アクセス
- BIG-IP Edge Portal による簡易なアプリケーション・アクセス
- 広範なクライアント・プラットフォームのサポート（iPad、iPhone、Mac、Windows、Linux、Android）
- ブラウザのサポート : IE、Firefox、Chrome
- サイト間の IPsec 暗号化
- アプリケーション・トンネル
- ユーザ ID に基づくダイナミック・ウェブトップ
- 保護されたワークスペース
- F5 Secure Web Gateway サービスによる Web フィルタリング、URL 分類、リアルタイムの Web マルウェア検出および保護、新たに出現する APT に対する独自のデータベース照合による脅威の検出と対策
- 認証方式 : フォーム、証明書、Kerberos SSO、SecurID、Basic、RSA トークン、スマートカード、N 要素
- エンドポイント検査 : Windows、Mac、Linux、ウイルス対策およびファイアウォール・チェック。Apple iOS および Google Android 対応のデバイスがジェイルブレイクされたり、root 化されていないかをチェックします。
- 数十のエンドポイント・チェック
- 仮想キーボードサポート
- カスタマイズしたログオンページ用のスタイルシート
- Windows Mobile パッケージのカスタマイズ
- Splunk による集中型の先進的レポート
- 仮想クラスタ・マルチプロセッシング（vCMP）

Solutions for an application world.

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

DS-15755 0214