SOLUTION BRIEF

FortiGSLB で あらゆるロケーションにアプリケーションを 迅速かつセキュアに提供

概要

エンタープライズおよびキャリアネットワーク向けにインターネットベースのサービスやソリューションの設計、導入を行う場合、水平方向へのスケーラビリティが重要になります。この種の企業は迅速かつ簡単に新しいネットワークリソースの追加やクラウドベースアプリケーションの導入を行うことで事業の継続性を確保しなければならないとともに、データセンターやサーバーに障害が発生した場合のスムーズなディザスタリカバリも必須となります。ところが、インターネット接続やセキュリティの信頼性が低いと、こうした作業は滞ってしまうことになります。

こうしたスケーラビリティや柔軟性が欠けていると、キャパシティの問題に対応する企業は、より強力なハードウェアデバイスにアップグレードせざるを得なくなります。このようなアップグレードはコストがかかり、フェイルオーバーやサービスの可用性の根本的な解決はなされないまま、TCO（総所有コスト）が大幅に増加してしまいます。

フォーティネットのGlobal Server Load Balancing (GSLB) Cloudは、企業がデータセンターから脱却し、新しいタイプのマルチテナントアーキテクチャに移行できるようにするDNSサービスで、ネットワークやインターネットベースのアプリケーションとサービスを迅速かつセキュアに提供します。

FortiGSLB でインフラストラクチャを簡単にスケーリング

アプリケーション環境の規模に関係なく、企業は追加のハードウェアを導入しなくてもアプリケーションを簡単に拡張できます。

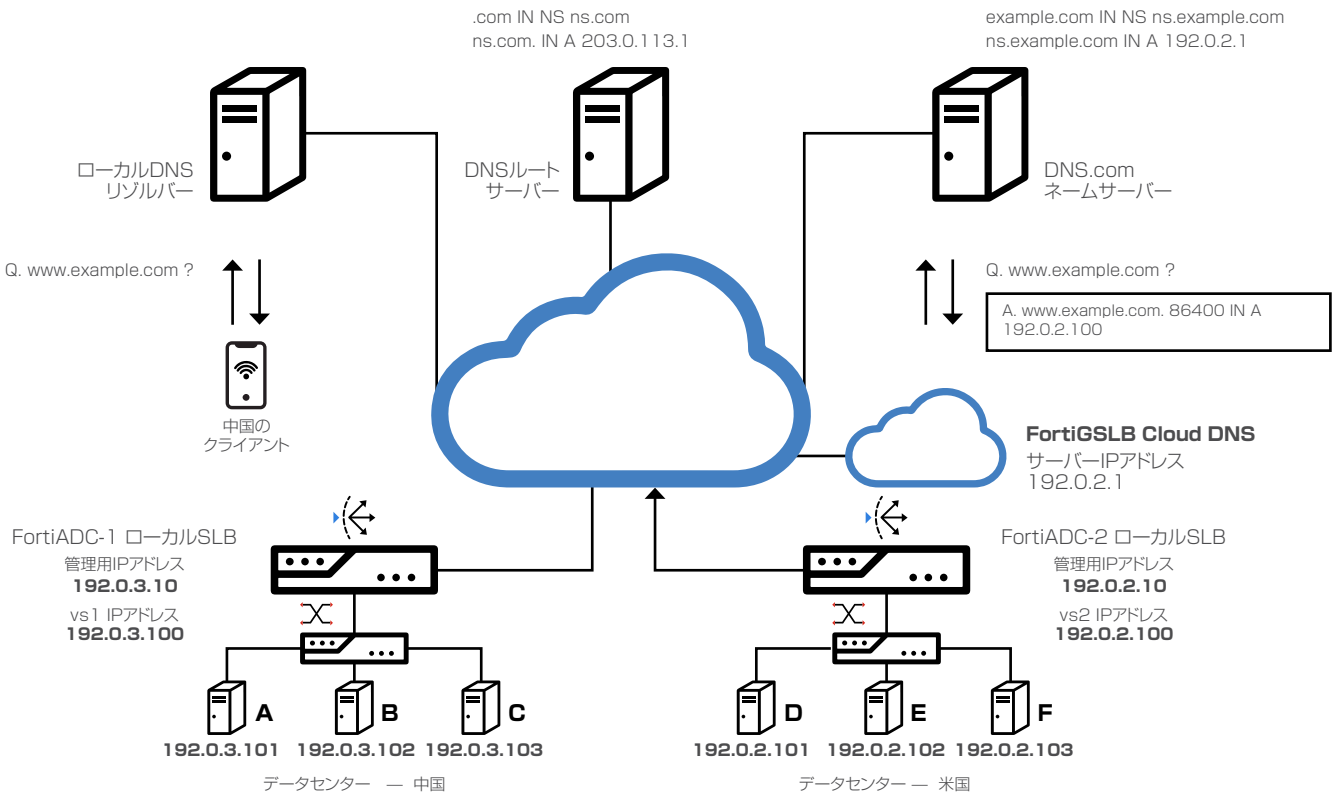

図1:FortiGSLB Cloud導入モデル

はじめに

FortiGSLBは、複数のデータセンターをまたいで増加し続けるリソースやアプリケーションがもたらす複雑さを軽減するクラウドベースのアプローチです。ディザスタリカバリを効率化し、パフォーマンス向上、アプリケーションデリバリのコスト削減を実現します。

従来のアプリケーションデリバリソリューションとは異なり、FortiGSLBは、常時稼働、常時可用を実現したホステッドGSLBソリューションを提供し、各データセンターにデバイスを設置する必要もありません。

使いやすいFortiGSLBインタフェースにより、ネットワークエレメント、ロケーション、サーバーパフォーマンス、カスタムポリシーに基づいて、各種ビジネス要件に合わせたルール設定が可能です。FortiGSLBは高度なヘルスチェックメカニズムも備えており、あらゆるロードバランシング要件やフェイルオーバーシナリオにも対応できるので、ミッションクリティカルなアプリケーションで100%のアップタイムを実現できます。

FortiGSLB は従来のデバイスベースソリューションをしのぐリーチと復旧力を備えたロードシェアリングとフェイルオーバー機能を提供します。

FortiGSLB のメリット

FortiGSLBが提供するルールベースの転送とヘルスチェックメカニズム機能は、以下のことを可能にします。

- **クライアントのインフラストラクチャを水平方向に拡大 ー** 複数のコロケーションや他の種類のデータセンター内にあるアプリケーションとサービスを使用することで、水平方向へのスケーラビリティが実現します。一か所に限定される垂直方向のスケーリングソリューションのような制約はありません。
- **すべてのフォーティネットアプリケーションとサービスを利用可能 ー** サービスレジリエンシを追加し、マルチテナントの事業継続計画（BCP）やディザスタリカバリ（DR）モデルのようなベストプラクティスを導入します。
- **レガシーデバイスのキャパシティ拡大 ー** FortiGSLB ではロードバランシングに「加重ラウンドロビン」によるアプローチを採用しており、よりパフォーマンスの高いデバイスを最大限利用することができます。
- **ベストパフォーマンスの確保 ー**地理的に最も近いソースを指示することで従業員やクライアントに最高のパフォーマンスを確実に提供します。
- **構築／開発 ー** 改善された新たな機能を構築または開発することができます。

以下の3つのシナリオの説明とソリューションでは、FortiGSLBとフォーティネットの他の製品、コンテンツデリバリネットワークを組み合わせて複数のデータセンターでのアプリケーションとサービスのスケーリング方法を解説しています。

ユースケース 1：FortiGSLB と FortiGate SSL/IPsec VPN によって信頼性とパフォーマンスの高い VPN を実現

テレワーカー向けにネットワークパフォーマンスを高めるべく、多くの企業がVPNエンドポイントを各地域に設置し、モバイルデバイスでの通信セキュリティを確立しようとしています。自宅、移動中、カフェなど、従来では考えられなかった環境で仕事をする従業員をサポートするために、社内ネットワークへのセキュアな接続は、その重要性を増しています。

小規模企業であれば単一のエンドポイントにVPNクライアントを設定してもかまいませんが、大規模な企業には移動の多い従業員のための堅牢なソリューションが必要です。複数の国で事業を展開している、あるいはその予定がある企業の場合は特にその必要性が高まります。ネットワークアクセスが不十分なために上級職の仕事が滞ることがよくあるからです。

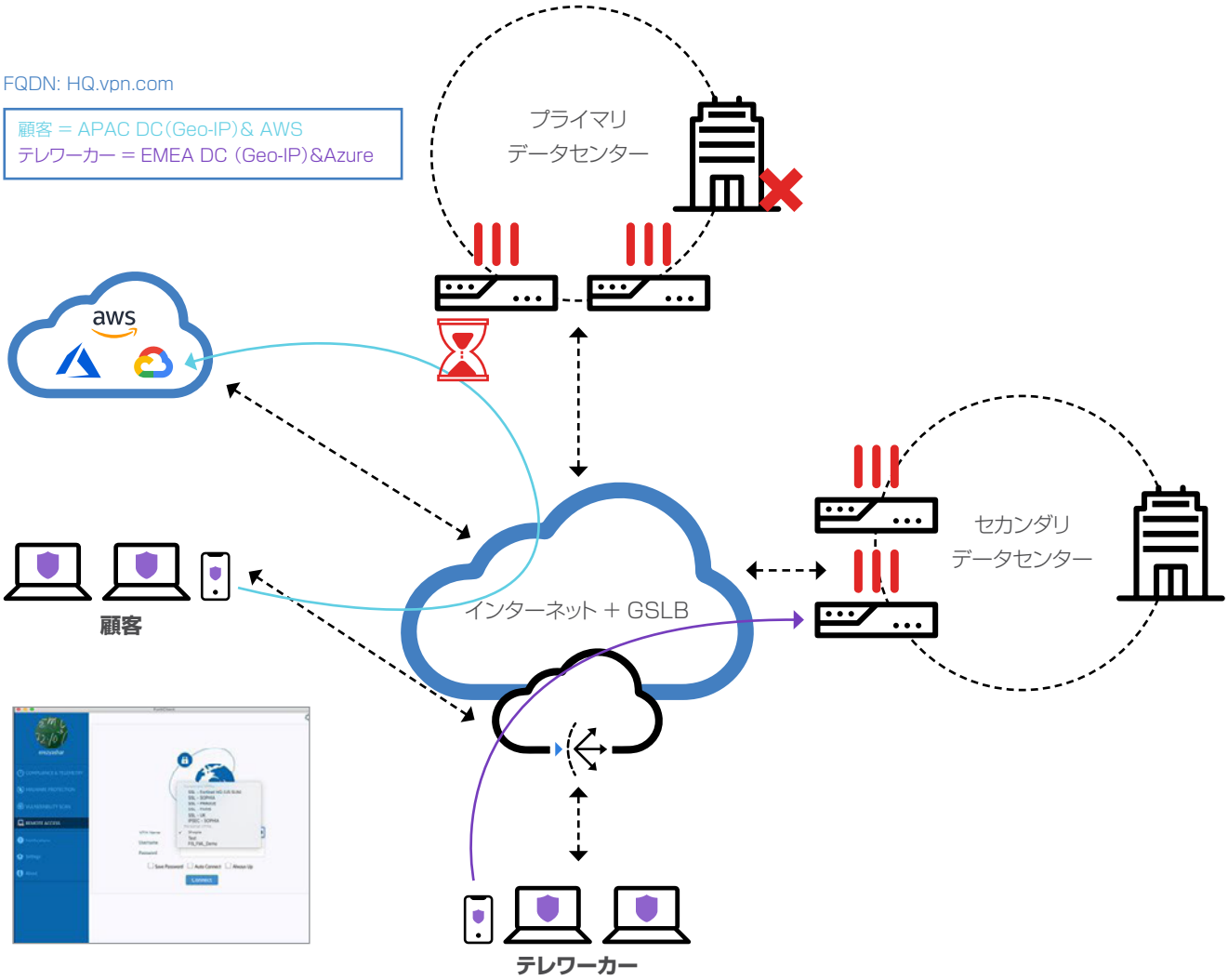

図2:FortiGSLBが障害のあるサーバーを検出してVPNトラフィックを転送

ソリューション

VPNのパフォーマンスとスケーラビリティを向上するために、モバイルクライアントを地理的に最も近いFortiGate VPNサーバーに自動的に接続するよう、FortiGSLBを設定することができます。

パフォーマンスは地理的な距離に比例します。最寄りのVPNサーバーに接続することで、顧客側のプライベートネットワークを経由して企業の各拠点間でEメールやインスタントメッセージなどのクライアントコミュニケーションが可能になります。さらにFortiGSLBのヘルスチェックメカニズムが応答のないVPNエンドポイントを自動的に除外するので、保守作業中もシームレスなユーザーエクスペリエンスを提供します。これによりVPN接続の信頼性が高まり、パブリックインターネット経由の場合に比べてレスポンスのよい通信が実現します。

ユースケース 2：FortiGSLB と FortiWeb の併用によって セキュアなウェブアプリケーションをあらゆるロケーションで提供

たとえば米国の西海岸にあるデータセンターにFortiWebデバイスが1台しかない企業が過負荷状態になった場合、東海岸、アジア、ヨーロッパのクライアントは深刻な遅延に見舞われます。FortiWebのアップグレードも1つの選択肢ですが、このソリューションでは海外顧客に対する遅延解消にはつながりません。該当する地域に複数のFortiWebを導入してFortiGSLBを利用するほうがよいでしょう。

FortiGSLB を FortiWeb と組み合わせることでウェブトラフィックを最寄りのデータセンターにルーティングするか、万が一データセンターやサーバーに障害が発生した場合はディザスタリカバリの措置を講じることができます。

ソリューション

FortiWebのウェブアプリケーションファイアウォールがウェブベースのアプリケーションとインターネットに接続されたデータを保護します。FortiGSLBは、FortiWebが増加することでより高度な柔軟性を顧客に提供します。たとえばFortiGSLBはデータセンターやサーバーの障害時には複数のFortiWebデバイス間で自動的にフェイルオーバーすることができます。あるいは地理的な距離やサーバーのパフォーマンスに基づき、クライアントを別なデータセンターに転送することもできます。

米国東海岸、アジア、ヨーロッパのデータセンターに3台のFortiWebデバイスを新たに設置し、合計4つの拠点で負荷を分散することで、当初のFortiWebデバイスはより優れたカスタマーエクスペリエンスを提供することできます。ヘルスチェックでいずれかのFortiWebアプライアンスに障害が検出された場合、FortiGSLBが別のルートにトラフィックを転送します。自動転送によってBCPやDR機能を高めると同時に、こうしたプロセスの複雑性を軽減することができます。

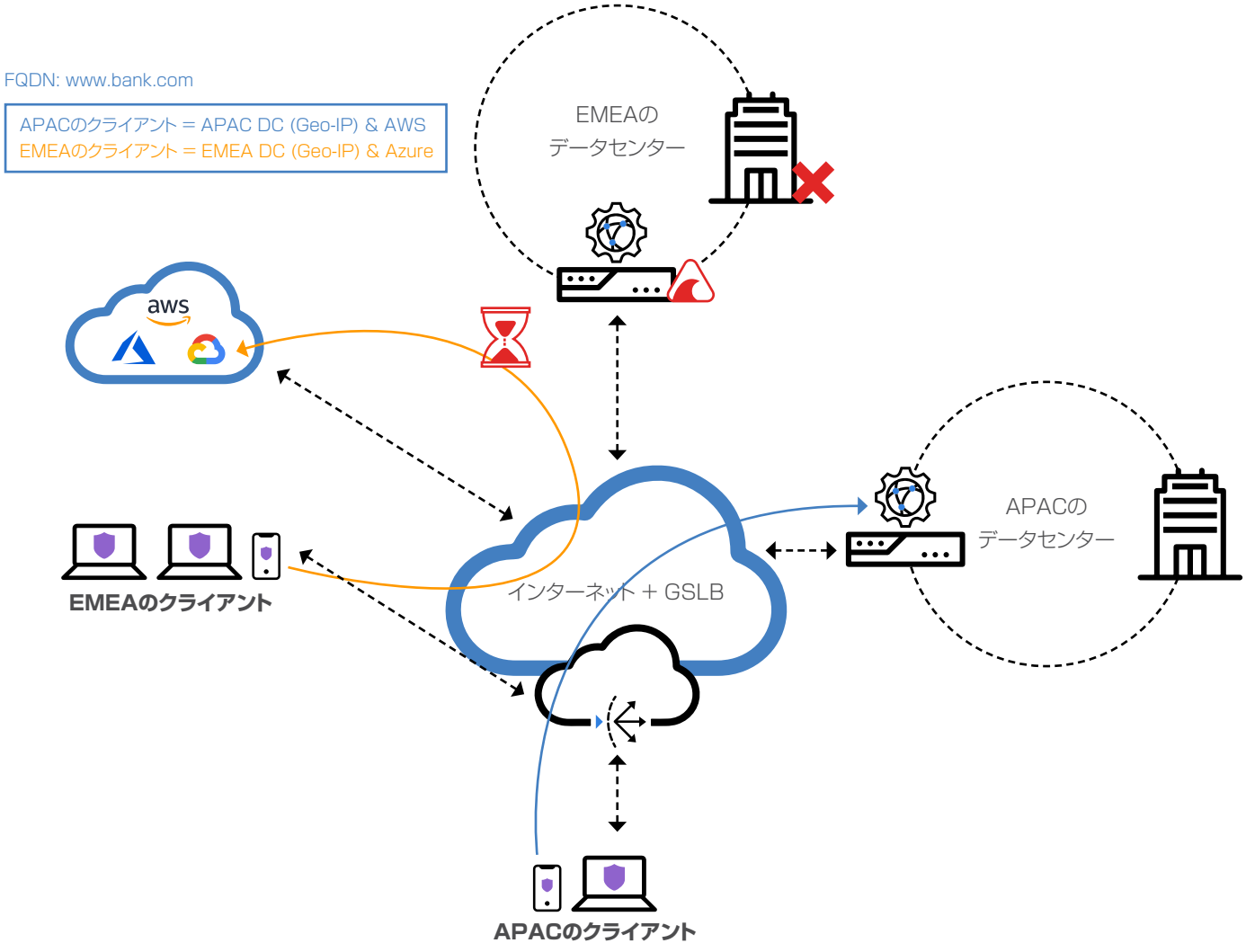

図3:FortiGSLBが障害のあるサーバーを検出してWebトラフィックを転送

ユースケース 3：マルチテナントメールサーバー向けの FortiGSLB と FortiMail を併用したフェイルオーバー構成

FortiMailの高可用性は、プライマリアプライアンスとバックアップ用のセカンダリアプライアンスという2つのアプライアンスをペアとして機能させることを可能にします。プライマリアプライアンスは接続とSMTP、POP、IMAPへのトラフィックを処理し、バックアップアプライアンスはプライマリアプライアンスが稼働している間は接続もトラフィックも処理しません。

このシナリオは社外サーバーから受信するEメールの処理に効果的です。ただし従業員の各メールクライアントがメールの送受信に単一のホスト名を使用していると、プライマリサーバーがオフラインまたは接続不能になった場合に問題が生じます。この場合、従業員はEメールへのアクセスや送信ができなくなり、業務が停止してしまいます。

FortiGSLB を FortiMail と組み合わせることで E メールの転送先を最寄りのデータセンターにルーティングするか、万が一データセンターやサーバーに障害が発生した場合はディザスタリカバリの措置を講じることができます。

既存のソリューションでは、企業側でmail.company.comのDNSエントリを変更または更新する必要があり、DNSレコードのTTL失効や反復DNSキャッシュが発生します。企業はEメールをGoogleアプリケーションなどのセキュリティの低いクラウドサービスに転送することもできますが、いずれの方法もEメールクライアントからバックアップサーバーへの転送が遅れ、生産性やサイバーセキュリティの低下につながります。さらに、企業がセカンダリEメールサーバーを別の場所に設置してインフラストラクチャの障害に対するセキュリティ強化をすることが非常に多くなっています。このシナリオでは、高可用性の機能が使えないことがあります。

ソリューション

FortiGSLBでヘルスチェックを行い、サーバーの可用性を確認します。サーバーが稼働していない場合は、FortiGSLBがユーザーを別のサーバーに自動転送してEメールを受信できるようにします。

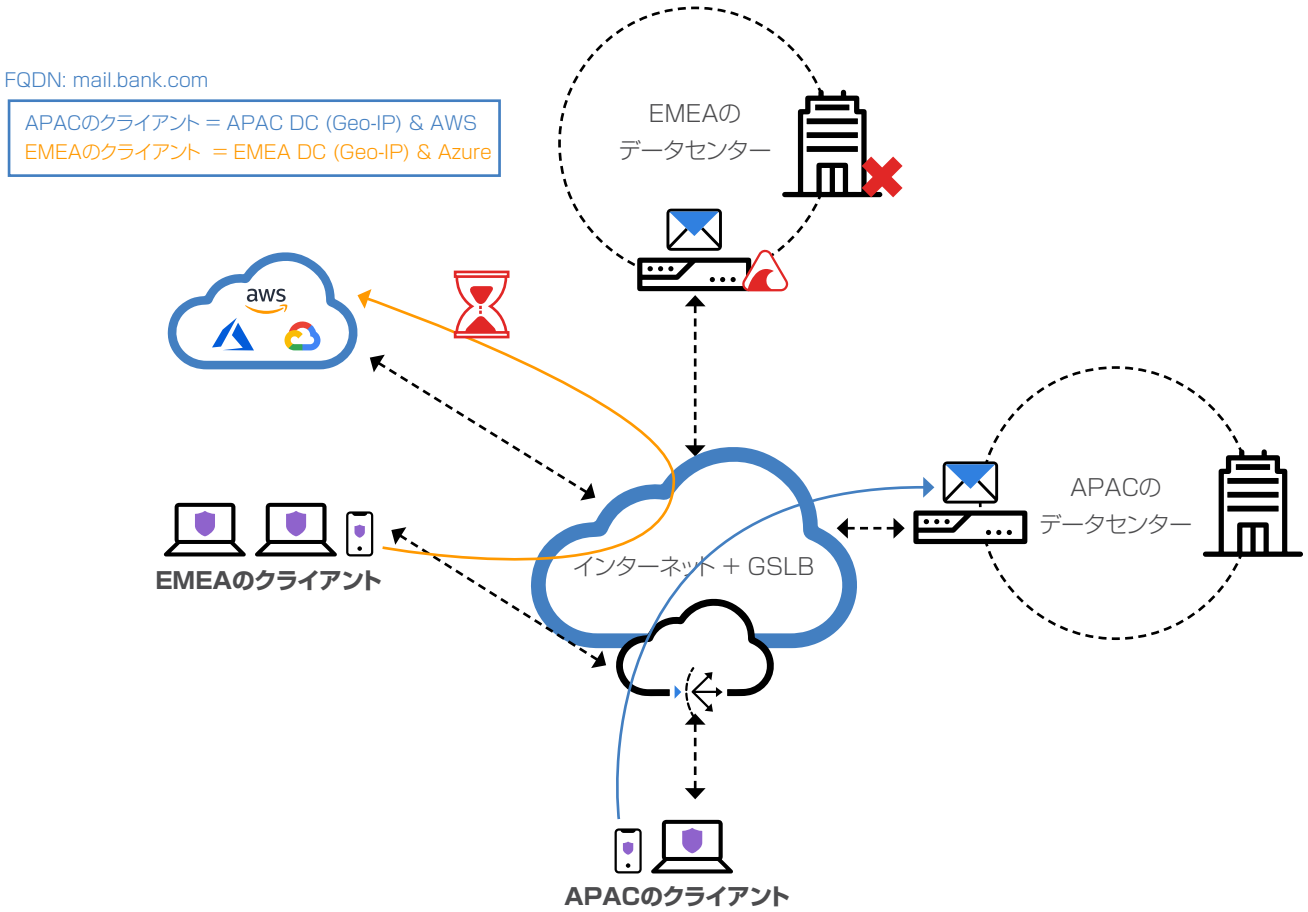

図4:FortiGSLBが障害のあるサーバーを検出してEメールを転送

結論

FortiGSLBは完全で管理しやすく信頼性の高いアプローチによって、ハードウェアをまったく追加することなく全世界の無数のデータセンターにウェブベースのアプリケーションを提供することができます。FortiGSLBを使用することで、企業はFortiMail、VPN、FortiWebをはじめとする他のフォーティネット製品のスケーリングが可能になります。こうしたシナリオや事例以外にもFortiGSLBでスケーラビリティや冗長性を実現できる方法は多く、アプリケーションデリバリで直面する課題に対処することができます。FortiGSLBに関する詳細や無料のデモをご希望の場合は、フォーティネットの営業担当者またはフォーティネットの認定リセラーにお問い合わせください。

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木7-7-7 Tri-Seven Roppongi 9階
www.fortinet.com/jp/contact

お問い合わせ

SB-k-FortiGSLB-2210-R1