ゼットスケーラーが MAN Energy Solutionsの ネットワークとアプリケーションの トランスフォーメーションを実現

MAN Energy Solutionsは、ドイツのアウクスブルクに本社を置く、船舶や定置用の大口径ディーゼルエンジンやターボ機械を提供する世界有数の企業です。同社が設計した2ストロークと4ストロークのエンジンは、自社での製造だけでなく、ライセンス生産もされています。
MAN Energy Solutionsは、ガスタービンの設計と製造も手掛けているほか、ターボチャージャ、プロペラ、ガスエンジン、化学反応器などの広範な製品に携わっています。

ゼットスケーラー導入の背景と課題

ビジネスのグローバル展開と並行して、輸送用の機械やシステムを搭載した、世界中に導入されるあらゆるサイズのエンジンやシステムに、IoTなどのテクノロジが急速に取り入れられるようになりました。また、企業規模の拡大とワークフォースがグローバルに変化するとともにモバイル化が進んでいることから、Webアプリやカスタムビジネスアプリケーションへの**モバイルアクセス**が必要とされるようにもなっています。

ネットワークとアプリの従来型の『城を堀で囲む』アプローチによる**セキュリティ**では、ワークロードがAWSやAzureへと移行した、インターネットが新しい企業ネットワークとなる最新のクラウド環境に対応できず、グローバルのスケーラビリティ、グローバルのアクセス、セキュリティポスチャを改善することはできません。このような環境で必要とされるのは、アプリケーションがインターネットに公開されないように、認証されたアクセスを使用して、信頼できるユーザを信頼できるアプリケーションに接続する方法です。

「エンタープライズ ITがモビリティとクラウドサービスの採用によって変化を遂げる中で、企業のアーキテクチャにも、あらゆる場所からあらゆるデバイスを使ってアクセスするユーザを保護するため、ニーズ拡大に対応した変化が求められています」

– トニー・ファーガソン氏
MAN Enegy Solutions
ITインフラストラクチャアーキテクト

MAN Energy Solutions（MAN）の懸念は、たとえ**スピードとアジリティ**を改善できる方法であっても、従来型のVPNソリューションによってアプリケーションにアクセスするやり方では、ユーザエクスペリエンスが低く、アプライアンスやソフトウェア、MPLSネットワーキングのコストが増えるために、クラウドの導入によるメリットが相殺されてしまうことでした。加えて、アプリがインターネット上で非公開になるようにセキュリティを強化したいとも考えていました。

「従来型のVPNを利用して、従業員がどこにいてもアプリケーションに接続できるようにしていましたが、低パフォーマンスという問題に加え、ユーザエクスペリエンスという面で社内から不満の声が上がっていました。当時のセキュリティスタンスでは、改善方法は見つからず、AWSとAzureの導入によって実現できるものでもありませんでした。オンプレミスのインフラストラクチャを管理する担当チームが社内にいるとはいえ、リアルタイム分析とアプリアクセスに必要なデータセットがニーズも含めて急増する中、対応するには小規模で不十分でした。加えて、高度な製品やテクノロジをグローバルに展開していたために、より多くのデータソースがオンラインになっていたほか、内部アプリケーションの刷新も図っていたので、こういったニーズへの対応がさらに困難なものになりました」（トニー・ファーガソン氏、MAN社ITインフラストラクチャアーキテクト）。

ゼットスケーラーを選択した理由

クラウドへの移行によって、MANは、ビジネスの課題の解決にあたっての確かなメリットを手に入れることができたと言います。「他社が続々とグローバル規模でクラウド実装に成功し、多くのユースケースを目にしたことから、自社のテクニカルな目標を解決できるアーキテクチャを特定することができました」（ファーガソン氏）。

MANがゼットスケーラーを採用したのは2011年。ユーザエクスペリエンスの向上、帯域幅コストの削減、厳しさを増すセキュリティの目標を達成するため、導入を決断しました。まずZIA（Zscaler Internet Access）を用いることで、世界中に分散するモバイルユーザをSaaSアプリケーションに接続することにし、更にはAPT（標的型攻撃）要件の解決にも、ゼットスケーラーを採用しました。さらには、ZPA（Zscaler Private Access）を導入することで、モバイルワーカや外注業者がオンプレミスで動作するアプリに時間や場所を問わずアクセスできるようにしました。直近では、AWSとAzureで動作するアプリのセキュアアクセスにもZPAを採用し、ネットワークコストの削減とモバイルユーザエクスペリエンスの向上を同時に実現することにも成功しています。

内部アプリケーションへのゼロトラストアクセス

ZPAは、VPNのコスト、複雑さ、セキュリティリスクに悩まされることなく、プライベートアプリケーションや資産へのポリシーベースの安全なアクセスを可能にする製品です。アクセス許可がないユーザに内部アプリケーションを「見せない」という考え方は、SDN（Software-Defined Network）と共に注目を集めるようになっていました。ゼロトラストモデルのアプローチでは、サービスが外部に公開されないため、アプリとユーザの両方をSAMLを使用して承認することで初めて、ユーザアクセスが確立されます。

メリット

- 優れたエンドユーザエクスペリエンスを提供
- ネットワークへのアクセス不要、アプリケーションアクセスを可能にすることで攻撃対象領域を削減
- 強力な認証ときめ細かいアプリケーションアクセスコントロールをグローバルで保証
- VPCの展開、安全なアクセスと管理が可能
- ユーザとアプリの最適パスを保証することでパフォーマンスの向上を実現
- アプリケーションやユーザのアクティビティの可視性が向上

「我々は、ゼロトラストモデル、あるいは**ブラッククラウド（SDP）**と呼ばれるモデルを実装することができました。このソリューションによって、攻撃対象領域を減らし、最新の安全なクラウドファーストのアプローチに置き換えることができました。さらには、ユーザ権限をきめ細かくコントロールできるようになったため、一人ひとりの従業員や外注業者がアクセスする必要のあるものだけにアクセスできるようになりました（ファーガソン氏）」。ネットワークではなく、アプリケーション単位でで外注業者のアクセスをセグメンテーションできるのがZPAの特徴です。

また、このアプローチによって、不正ソフトウェアの水平移動も防ぐことができます。クライアントからサーバへのアクセスを可能にしつつ、その逆は許可しないよう設定することが可能です。これらふたつのパラダイムを組み合わせることで、すべてのセッションの検証が完了してからアクセスが許

可されるため、悪意ある水平移動が阻止されます。ゼロトラストモデルを前提に、ユーザ認証、承認、既知と未知のアプリケーションに基づいてポリシーを適用することで、セキュリティを強化できます。

世界規模でユーザを接続する最新のアプローチ

MANがゼットスケーラーを導入した背景には、ビジネスアプリや開発プロジェクトのクラウドへの移行、クラウドサービスの増加、世界中に分散する多くの従業員やパートナーへ早急なアクセス提供が求められていたという社内的な事情があったと言います。エンドユーザを自社アプリに接続する、より高速で安全な方法を必要としていた中、従来のVPNアプローチから脱却できなければ、ITとネットワークの両方のリソースの負担が増大する結果となってしまうことを理解した上で、ビジネスの柔軟性と俊敏性を向上させるべく、ゼットスケーラーのクラウドセキュリティの導入を図ったと言います。

ゼットスケーラーのクラウドは、リモートアクセスへの従来のハードウェアやソフトウェアのセキュリティスタックの必要性を排除できる、強力で優れた代替手段です。移動中のエンドユーザによるVPNクライアントやリモートアクセスのヒューリスティックを解消し、トラフィックの代替パスを提供するほか、インターネットベース接続のMPLSトンネルの必要性を最低限に抑えることができます。

スピード、アジリティ、パフォーマンスの向上

結果、MANは複雑な管理とコストを同時に低減させることができ、エンドユーザエクスペリエンスを向上させ、アプリケーションがデータセンタあるいはクラウドのどちらで動作する内部アプリケーションであっても、クラウドと同様のシームレスなユーザエクスペリエンスが提供される環境を実現させました。ユーザは従来のリモートアクセスチョークポイントを完全にバイパスし、ゼットスケーラーのグローバルクラウド経由でアプリケーションにそのままアクセスするため、アプリケーションのホスティング場所に完全な柔軟性が提供されるほか、TLSベースの暗号化されたマイクロトンネル接続によって機密データは保護されます。ユーザがネットワークに接続することも、アプリケーションが未承認のユーザに公開されることもありません。従来のソリューションで悩まされることが多い複雑さもクラウドで軽減することができたと言います。

また、VPNインフラストラクチャとソフトウェアのライセンスが不要になったことで、2桁のコスト削減率を実現し、帯域幅コントロールによってミッションクリティカルトラフィックをWebの閲覧などの優先度の低いトラフィックより優先させることで、ネットワークパフォーマンスの向上にも成功しました。

最大な技術的メリットのひとつは、攻撃対象領域を抑え、すべての管理の保護をAWSとAzureに集約できる点です。MANは、ZPAのログ・分析クラスタをSIEMへのログストリーミングに利用することで、ユーザアクセスとアクティビティの可視性を強化しています。

「新しいVPCの導入と新しい名前空間を作成するのに必要なのは、ほんの数分です。名前空間のルーティングを使用できるため、IPではなく、名前空間に基づいてトラフィックをコントロールできることは、我々にとって大きなメリットです。結果として、効果的なポリシーを作成できるようになり、ネットワークのコストと複雑さを減らすこともできました。コンサルタントのオンボーディングプロセスもはるかに速くなり、数週間ではなく数時間以内のオンボーディングが可能になっています」（ファーガソン氏）。

ゼットスケーラーについて

ゼットスケーラーは2008年に、「アプリケーションのクラウド移行に伴って、セキュリティもクラウドに移行する必要がある」という、シンプルで力強い概念に基づき設立されました。ゼットスケーラーは現在、世界中の数千の組織のクラウド対応の運用への移行を支援しています。

ゼットスケーラー株式会社
東京都千代田区大手町1-9-2
大手町フィナンシャルシティ
グランキューブ 3階
www.zscaler.jp