ソリューション概要

通信
DDoS 攻撃からの防御

SmartNIC 対応 F5* BIG-IP* VE とインテル® FPGA PAC N3000 がクラウド環境での大量 DDoS 攻撃を阻止

サービス・プロバイダーや企業を対象に 5G サイバー攻撃の脅威軽減を自動化

5G インフラストラクチャーへの移行に伴って、新たな DDoS 攻撃のリスク増大が懸念される中、このような攻撃は規模も大きく、深刻さや複雑さの度合いが高まると予測されます。5G インフラストラクチャーを構築するサービス・プロバイダーは、帯域幅や加入者への影響を緩和するために、戦略を立てなければなりません。

幸い、より高度な仮想化テクノロジーへの移行が進み、サービス・プロバイダーは DDoS 攻撃の効力と影響をより素早く、大規模に抑え込めるようになっています。例えば、FPGA ベースのスマート NIC であるインテル® FPGA PAC N3000（インテル® FPGA プログラマブル・アクセラレーション・カード N3000）とともに組み込まれた F5 の SmartNIC 対応 BIG-IP* Virtual Editon（VE）ソリューションも、その可能性を実現する 1 つです。サービス・プロバイダーのネットワークは、このソリューションを一般的な市販（COTS）のサーバーを使用する仮想化 5G インフラストラクチャーと組み合わせることによって、ユーザーのアプリケーションやサービスへのアクセスに悪影響を及ぼしかねない、進化し続ける DDoS のボリューメトリック型攻撃を自動的に検出し、現行の手法よりも迅速かつ的確に防御することができます。

こういった新種の DDoS 攻撃に対抗する必要性に迫られているのは、サービス・プロバイダーに限らず、デジタル変革のさなかにある企業や組織も同様です。ここで説明するソリューションは、そのような企業にも同等の保護を提供します。

現在製造中で利用可能な多くの Tier 1 サーバーの OEM では、それぞれのサーバーに FPGA カードを認定しています。FPGA カード搭載サーバーの最新リストについては、こちらをクリックしてください。インテル® FPGA PAC N3000 は動的な構成が可能で、5G vRAN、Open vSwitch*、セグメント・ルーティング v6、Tungsten Fabric、5G User Plane Function（UPF）、vBNG、セキュリティー・ソリューションなど、複数のワークロードを高速化します。これによって、サービス・プロバイダーは、インテル® FPGA PAC N3000 搭載のサーバーを導入して、エッジで求められるサービスに応じたさまざまなクラウドネイティブのネットワーク機能や仮想アプライアンスを実装することができます。

妨害目的の巧妙な DDoS 攻撃は防御が困難

DDoS 攻撃は、報復、抗議、傍受 / 盗用、脅しといった標的を絞った行為からいたずらまで多岐にわたりますが、どれも目的は等しく、サービスの提供を妨害し、企業の稼動能力が落ちるよう仕向けるものです。

攻撃者の技量次第で、簡単に手に入る DDoS ツールを利用したり、カスタマイズした高度な攻撃を仕掛けてくることもあります。通常、そのような攻撃は次の 4 つのタイプが組み合わされています。

- **ボリューメトリック型：**レイヤー 3、4、7 を狙うフラッドベースの攻撃（ほとんどの場合ボットネットを使用）
- **非対称型：**タイムアウトまたはセッション状態の変化を誘引
- **演算処理型：**CPU とメモリーを消費
- **脆弱性ベース：**アプリケーション・ソフトウェアの脆弱性を悪用

損害レベルが最大級の DDoS 攻撃は、ほとんどの場合、迂回路を作るためのボリューメトリック攻撃とアプリケーション固有の攻撃を組み合わせており、実際の標的を見極めるのは困難です。このようなタイプの複雑な攻撃は防御が難しく、さらに高度で持続的な脅威が来ることを示唆している場合があります。

攻撃を迅速に検出して阻止しない限り、サービス・プロバイダーはサービスの継続性も加入者の満足度も維持することはできません。サービス・プロバイダーにレイヤー 3 ~ 7 向けの包括的かつ高性能の DDoS ソフトウェア緩和ソリューションを提供するのが、F5 の SmartNIC 対応 BIG-IP* VE ソリューションです。この高性能でステートフルなオンプレミスのフルプロキシー・ネットワーク・セキュリティー・ソリューションは、最も広く導入されているプロトコルを介してネットワークに侵入するネットワーク攻撃、アプリケーション攻撃、ボリューメトリック攻撃を緩和する F5 の Silverline* クラウド DDoS スクラビング・サービスを組み合わせることもできます。

攻撃テストの結果

F5 が実施したテストでは、インテル® FPGA PAC N3000 とともに実装された SmartNIC 対応 BIG-IP* VE ソリューションは、COTS サーバーのソフトウェアでの処理と比較して、最高で 300 倍高いレベルの DDoS 攻撃（IP フラグメント攻撃）に耐えました。このソリューションは、「問題のない」トラフィックを取り込みつつ、「問題のある」攻撃トラフィックを検出してブロックしました。[1]

構成の詳細については、脚注 1 を参照してください。性能やベンチマーク結果について、さらに詳しい情報をお知りになりたい場合は、http://www.intel.com/benchmarks/（英語）を参照してください。

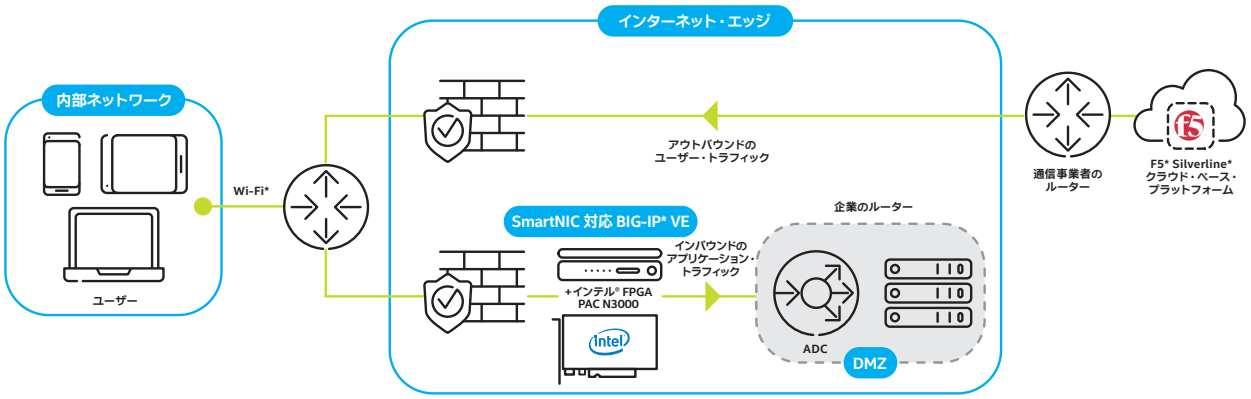

図 1. 巧妙な DDoS 攻撃からサービス・プロバイダーを保護する F5 ソリューション

このオンプレミスのプラットフォームは、専用に構築された F5 のソフトウェアおよびクラウド向けスクラビング・サービス（名称：F5* Silverline* DDoS Protection）と組み合わせることで、事後対応型と予防型の両方のハイブリッド DDoS 防御を提供します。2 つの組み合わせによって、攻撃をリダイレクトしてデータセンターから遠ざけ、クラウドベースで緩和し、常時稼動サービスを持続できます。

F5 はインテルと連携して、インテル® FPGA PAC N3000 を SmartNIC 対応 BIG-IP* VE とともに一般的な市販（COTS）のサーバーに搭載するソリューションを開発しました。DDoS 特有の機能を CPU から SmartNIC FPGA に移すことによって、CPU が解放され、設計で意図したパフォーマンスに従事できるようになります。FPGA は、違ったタスクを素早く実行するようプログラムすることも可能です。F5 ソフトウェアの今後のリリースでは、さらなるオフロード機能を FPGA 内で高速化することが可能になり、幅広い高性能ユースケースに対するシステムの柔軟性を向上します。

目的に特化して構築されたソフトウェアの組み合わせとインテル® FPGA PAC N3000 により、SmartNIC 対応 BIG-IP* VE ソリューションは、サービス・プロバイダーや企業にデータセンター内の仮想アーキテクチャーやソフトウェア・ベースのアーキテクチャーに、最適な NFV ファイアウォール /DDoS 防御を提供できるよう設計されています。また、サービスやアプリケーションを保護する専用のカスタム・ハードウェアと同等の機能も提供します。

これは、ネットワーク脅威に関するインテリジェンスとマシンラーニングによるパケットベースの解析を適用することによって、演算サイクルを最小限に抑えながら、大規模なネットワーク攻撃をより効率的にブロックすることができ、TCO を 4 年間で約 47% 低減する[2] CPU 効率の高いソリューションとなっています。また、SmartNIC に組み込まれる拒否リスト / 許可リストの更新もサポートしており、日々変化する脅威の状況に対し最新の対策を行うことができます。

DDoS 攻撃を防御するため、このソリューションを新しい領域やエッジに近いところに導入すれば、サービス・プロバイダーは、現行のテクノロジーでは見つけにくいサイバー脅威や攻撃を可視化できるようになり、自動化と組み合わせることで、総保有コストを抑えつつ、ネットワークを攻撃から防御しやすくなります。

クラウドと 5G 向けの DDoS 攻撃の緩和

SmartNIC 対応 BIG-IP* VE は、5G アーキテクチャーを構築するサービス・プロバイダーに、クラウド環境対応の卓越した DDoS 緩和機能を提供し、次のことを実現します。

- サービスの可用性の向上とレイテンシーの低減
- パフォーマンスを損なうことなく、ハードウェアからソフトウェアへの迅速な移行を促進
- サービス停止に関連する収益損失を回避しながら、拡張性と CPU 効率により運用コストを削減

詳細情報

インテル® FPGA PAC N3000 の詳細については、
http://www.intel.co.jp/pacn3000/ を参照してください。

F5 のセキュリティー専門家へのお問い合わせ ›

F5 の紹介

F5（NASDAQ：FFIV）は、アプリケーションを開発段階からライフサイクル全体にわたって、あらゆるマルチクラウド環境で強化し、大企業、サービス・プロバイダー、政府機関、消費者向けブランドなど、F5 のクライアントが差別化した高性能の安全なデジタル体験を提供できるよう支援しています。詳細については、https://www.f5.com/ja_jp を参照してください。また、F5 とそのパートナーおよびテクノロジーの詳細については、Twitter* で @f5networks のフォロー、または LinkedIn*、Facebook* のページで参照できます。

F5 Networks, Inc.
801 5th Avenue
Seattle, WA 98014
888-882-4447
f5.com

[1] F5 社内テストに基づく。Ixia 製トラフィック・ジェネレーターを使用して、「問題のない」トラフィックと「問題のある」トラフィックの両方をシミュレーションし、インテル® FPGA PAC N3000 上で DDoS 防御を有効にした結果と、BIG-IP* AFM VE ファイアウォールをソフトウェアのみで実行した結果を比較。テスト構成：Supermicro* SYS-1019P-WTR、CPU：インテル® Xeon® Gold 6240 プロセッサー @2.60GHz（18 コア /36 スレッド）、KVM バージョン：1.5.3、ベース OS：CentOS* Linux* リリース 7.7.1908（コア）、インテル® FPGA PAC N3000 SmartNIC x1、ファイアウォール SW：BIG-IP* Advanced Firewall Manager Virtual Edition（VE）v15.1.0.4。トラフィック生成の構成：問題のあるトラフィック：Ixia IxExplorer IxOS 8.5.1700.5 EA.Ink、問題のないトラフィック：IXIA XGS12。

[2] ハイパフォーマンス（24vCPU）BIG-IP* VE AFM ライセンスに年間サポート費を加えたコストと、SmartNIC 対応 BIG-IP* VE ソリューション（ハイパフォーマンス 8vCPU VE AFM、インテル® FPGA PAC N3000 の価格、F5* SmartNIC アドオンライセンス、年間サポート費）4 年間分のコストを比較して算出した割合。

344445-001JA