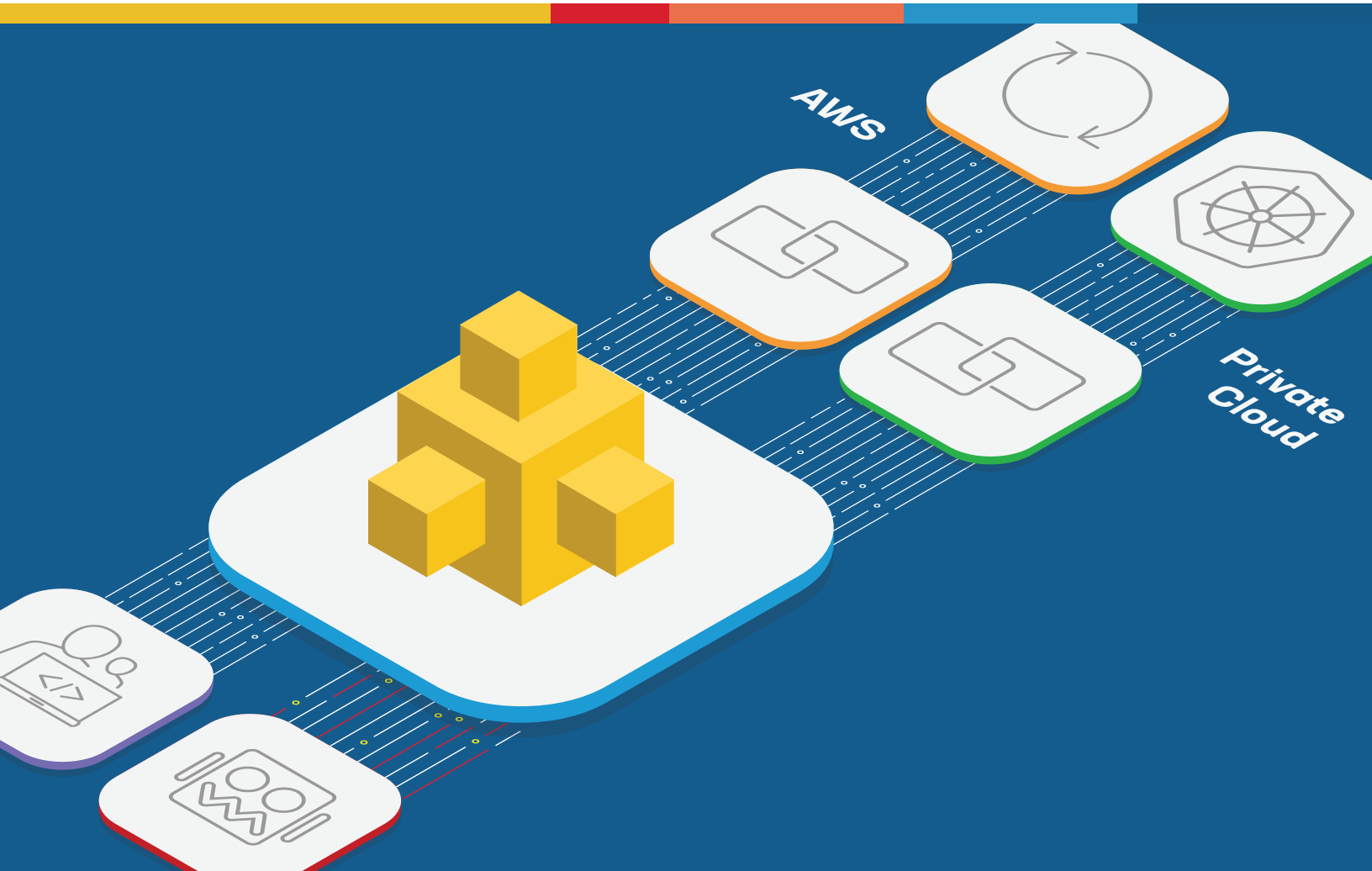
ソリューションの概要

分散型クラウドによる DDoS 攻撃緩和

F5 Distributed Cloud DDoS Mitigation は、企業やホスティングサービスプロバイダに対する L3-L7 攻撃から保護するための、DDoS および高度なセキュリティサービスを提供します。



主な利点

稼働率の最大化
F5 のグローバルネットワークとサポートを活用することで、高度なボリューム型攻撃や分散攻撃から、重要なアプリケーションとインフラストラクチャの可用性を守ります。

総運用コストの削減
クラウドベースのネットワーク境界セキュリティに移行することで、アプライアンスやレガシーアーキテクチャへの依存を減らし、CapEx と OpEx を削減します。

オンデマンドのスケーラビリティ
データセンターにアプライアンスやネットワーク容量を追加することなく、オンデマンドで動的に容量を拡張し、新しいサービスを導入できます。

生産性の向上
SaaS ベースのセキュリティプラットフォームと単一画面により、ネットワークと DevOps を強化します。既存のリソースで、より多くのプロジェクト、新しいアプリケーション、および容量の拡張に対応します。

この 10 年間で分散型サービス拒否（DDoS）攻撃の量と複雑さは急増し、これが懸念材料となるだけでなく、最も洗練された防御策を見つける理由となっているのも当然のことです。F5 Labs によると、2021 年 3 月までの 15 か月間で DDoS 攻撃は 55% 急増し、さらに複雑になり、54% のインシデントが複数の攻撃ベクトルを利用していました。

DDoS 攻撃の傾向に関する F5 のレポートによると、この期間の最大の攻撃は 500Gbps を計測し、5 つ以上の異なる攻撃ベクトルを使用していました。技術分野は、最も多く標的とされ、この 15 か月間で DDoS 攻撃全体の 27% を受けていました。

重要なネットワークやアプリケーションのリソースを消費しようとするボリューム型 DDoS 攻撃は、全インシデントの 73% を占めていました。

しかし、脅威アクターは、ネットワークとアプリケーションスタックの異なるレイヤーを悪用しようとすることも増えています。アプリケーションへの攻撃は、以前に比べて急増し、これらの DDoS 攻撃の 16% で確認されています。

今日、DDoS 攻撃緩和は不可欠であり、ソリューションの品質と範囲が重要です。ネットワークとアプリケーションのエコシステム全体で複数のレイヤーに対する攻撃から保護する必要があります。

F5® Distributed Cloud DDoS Mitigation は、F5 の SaaS ベースの Web Application and API Security（WAAP）ソリューションの主要製品で、カスタム DoS ルールや、エッジファイアウォールによるトラフィックの事前スクリーニングから、企業やホスティング / サービスプロバイダ向けの高度なスクラビングによるディープパケットインスペクションまで、複数の保護レイヤーにより、L3-L7 におけるさまざまなサービス拒否攻撃を軽減します。

大容量、クラウドベース、ハイブリッドな DDoS 攻撃緩和

脅威アクターは、ネットワークとアプリケーションスタックの異なるレイヤーを悪用しようとすることが増えています。アプリケーションへの攻撃は、以前に比べて急増しました。

DDoS 攻撃から保護するために、F5 Distributed Cloud DDoS Mitigation は、Tier-1 IXC に導入された接続拠点（PoP）が専用のマルチテラビット冗長プライベートバックボーン上で相互接続された、グローバルにセキュアなネットワークを活用します。F5 の PoP は、DDoS 攻撃緩和、L3 ファイアウォール、異常検知など、クラウドネットワークベースの堅牢なインフラストラクチャ保護を提供します。

主な特徴

マルチレイヤーのグローバル DDoS 保護
DDoS 攻撃緩和システムは、世界中の F5 の PoP に分散され設置されていて、L3/L4 および高度な L7 攻撃を攻撃源に最も近い場所でフィルタリングします。

大容量防御
F5 のセキュアなバックボーンとスクラビングインフラストラクチャは、12Tbps 以上のスクラビング容量により、今日の最大かつ最も複雑な DDoS 攻撃にも対応できるように設計されています。

一元的な可観測性
F5 Distributed Cloud Console は、一元管理を実現し、脅威の可視化とリアルタイムな軽減データによりカスタマイズが可能です。

あらゆる規模の顧客をサポート
F5 のオンデマンドキャパシティは、BGP 直接接続や GRE トンネルなど、あらゆる規模の顧客のニーズをサポートします。

継続的な攻撃監視 / 軽減
F5 のテクニカルアシスタンスセンターは、24x7 体制で稼働し、攻撃を受けても事業継続できる高いディペンダビリティを備えています。

クラウドベースの DDoS 攻撃緩和

Distributed Cloud DDoS Mitigation は、企業やサービスプロバイダのネットワークインフラストラクチャと Web アプリケーションサービスの両方を DDoS から保護します。F5® Distributed Cloud Mesh は、F5 の PoP 上で稼働し、ネットワークとアプリケーションの両方のトラフィックに対してインテリジェントな軽減ソリューションを提供して、顧客のインターネットアクセスのアップストリームに導入されます。パブリックアクセスを利用した DDoS 攻撃から自律的に保護します。

F5 のグローバルに導入された大規模なネットワークインフラストラクチャにより、Distributed Cloud Mesh は、Generic Routing Encapsulation（GRE）トンネルに加えて、Border Gateway Protocol（BGP）直接接続もサポートしています。この DDoS 攻撃緩和システムは、F5 の世界中の PoP に分散されていて、攻撃源に最も近い場所で（オンデマンドまたは常時サービスで）L3/L4 および高度な L7 攻撃をフィルタリングします。

ハイブリッド DDoS 攻撃緩和

オンプレミスの防御と F5 のクラウドベースの DDoS 攻撃緩和を組み合わせることで、ネットワーク層とアプリケーション層を狙った攻撃に打ち勝つための制御が可能になります。このアプローチは、複数の IP トランジットプロバイダの運用環境でオンプレミスのアプライアンスの処理能力を超える大規模な DDoS 攻撃から防御する手段として適しています。

オンプレミスのアプライアンスやインターネットリンクの容量を超えるボリューム型攻撃が発生した場合、管理者は、API コールを介して、または F5® Distributed Cloud Console で直接、DDoS 攻撃緩和を有効にできます。攻撃を受けている IP プレフィックスが、F5 によってアナウンスされ、軽減されます。スクラビングされたトラフィックは、直接の BGP ピアリングまたは GRE トンネリングを通じて、F5 Distributed Cloud Services から受信されます。

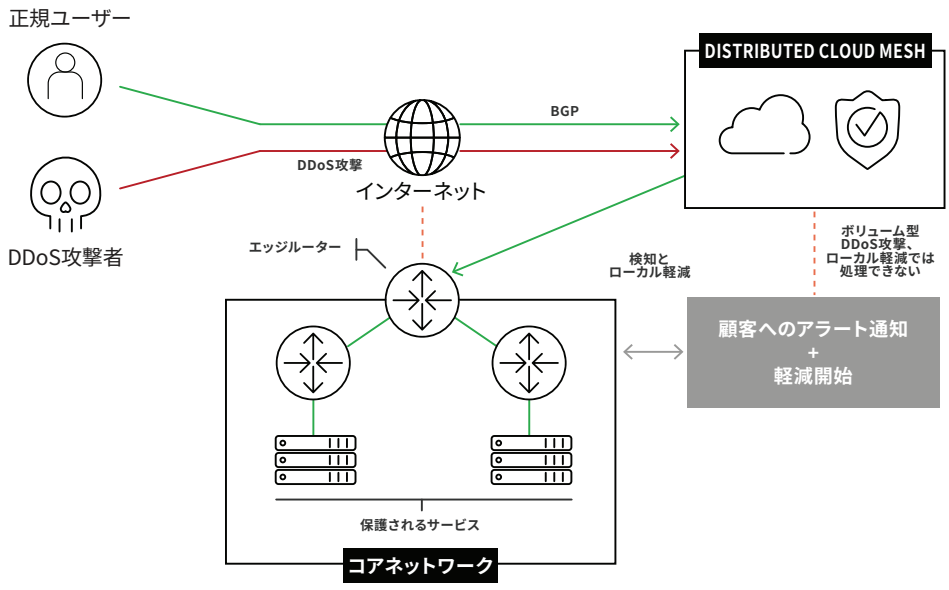


図 1：ハイブリッド DDoS 保護：クラウド軽減

F5 の DDOS 攻撃軽減システムは、F5 の世界中の POP に分散されていて、攻撃源に最も近い場所で L3/L4 および高度な L7 攻撃をフィルタリングします。

まとめ

F5 Distributed Cloud のセキュアなバックボーンは、3Tbps を超える今日の最大かつ最も複雑な DDoS 攻撃に対応できるように設計されています。攻撃が始まると、Distributed Cloud Mesh は以下のアクションを実行します。

1. クラウド検知
F5 のクラウド検知装置とソフトウェアが攻撃を検知します。検知は、ボリューム型攻撃などの静的なルールと、顧客ごとにパーソナライズされたルールを組み合わせて行われます。

- Distributed Cloud Mesh ルーターは、NetFlow 情報を Distributed Cloud NetFlow コレクタとアナライザに送信します。
- NetFlow のリアルタイムのポーリングと情報収集（送信元 | 送信先 ASN、IP アドレス、ネクストホップ IP | ASN など）により、クラウド検知はアラートを見逃しません。

2. 顧客へのアラート通知
攻撃が検知されると、24/7/365 体制の SecOps チーム（Security Operations Center）はアラートを受け取り、顧客に通知して軽減を開始するか、顧客に代わって軽減を開始します。

3. Cloud-Based DDoS Scrubbing
Cloud-Based DDoS Scrubbing の顧客は、アプリの場所、サービスレベル、必要な保護に応じて、さまざまなサービスおよび接続性オプションを使用できます。たとえば、常時稼働または常時利用可能なスクラビングオプションや、BGP または DNS ベースのリダイレクト、直接接続またはピアリング経由など、スクラビングのための複数のルーティングオプションがあります。

BGP アナウンスメントを変更し、他のトランジットプロバイダではなく、Distributed Cloud Mesh を経由してトランジットを誘導できます。Distributed Cloud Services は、BGP とスクラビングセンターを使用してトラフィックを誘導し、攻撃をブロックして、正規のトラフィックのみを通過させることができます。

F5 Distributed Cloud DDoS Mitigation および Distributed Cloud WAAP サービスについて詳しくは、f5.com をご覧ください。詳細またはデモの予約については、sales@f5.com までお問い合わせください。

DC0122 | OV-XC-830153919