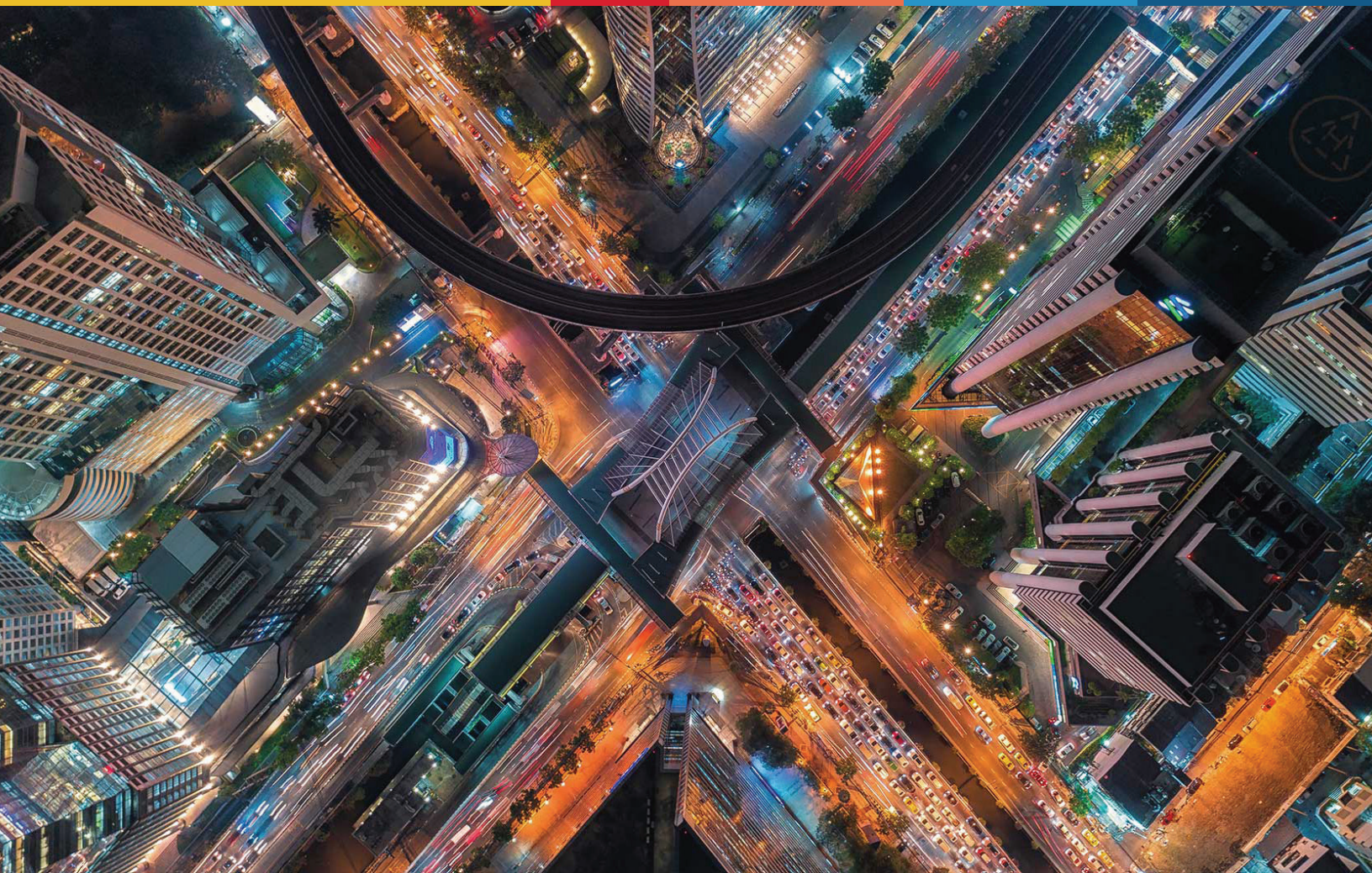
F5® Distributed Cloud DDoS Mitigation

Managed Service

F5 Distributed Cloud DDoS Mitigationは、ネットワークとアプリケーションを標的とした大規模なボリューム型攻撃をリアルタイムで検知および緩和して、攻撃トラフィックが毎秒数百ギガビットを超える可能性のあるマルチベクトルのサービス拒否アクティビティからお客様のビジネスと顧客を守るSaaS型のマネージドサービスです。



主な利点

DDoS 攻撃中でもビジネスをオンライン状態に維持
DDoS 攻撃が企業ネットワークに到達してビジネスに影響を与える前に、クラウドのリアルタイムの DDoS 攻撃検知および緩和機能を使用して DDoS 攻撃を阻止します。

すべての DDoS 攻撃ベクトルから迅速に防御
すべての攻撃ベクトルに対するマルチレイヤーの L3 ～ L7 の DDoS 攻撃防御により、DDoS 攻撃の脅威に迅速に対応し、攻撃を緩和します。

攻撃対策に関するインサイト
F5 Distributed Cloud Services カスタマーコンソールは、攻撃の前後および攻撃中でも攻撃対策に関する透過的な可視化およびレポートを提供します。

ボリューム型攻撃防御
数テラビット規模の能力を特徴とする業界をリードする DDoS 攻撃緩和を使用して、最大規模の DDoS 攻撃からでもビジネスを保護します。

SaaS 型、グローバルに利用可能、ビジネスへの影響も最小限
F5 のグローバルネットワークを利用することで、業務に影響を与えず、ハードウェアやソフトウェアに追加投資することなく、クラウド DDoS 防御を迅速に導入できます。

専門家によるサービス
F5 の SOC（セキュリティオペレーションセンター）のセキュリティエンジニアが、24x7 体制でお客様をサポートし、アップタイムと DDoS 攻撃への対応に関する最適なサービス SLA を提供します。

F5 Distributed Cloud DDoS Mitigation は、DDoS 攻撃をリアルタイムで検知および緩和する SaaS 型マネージドサービスオプションです。F5 のセキュリティオペレーションセンター（SOC）は、24x7 体制のグローバルサポートを提供しています。F5 の SOC のセキュリティエンジニアは、お客様のアプリケーションの継続的な可用性をサポートします。

F5 Distributed Cloud DDoS Mitigation が活用するネットワークでは、スクラビングデータセンターでホストされるリージョナルエッジ（RE）が、ティア 1 キャリアが運用するマルチテラビットの冗長な専用プライベートバックボーンで相互接続され、グローバルなセキュリティが確保されています。可用性に優れたグローバルなスクラビングセンターとネットワークは、DDoS 攻撃の発信源のより近くでトラフィックを遮断することで、単一のスクラビングセンターでは圧倒されるリスクを軽減します。現在のスクラビングセンターと運用状況の一覧について、F5 Distributed Cloud Status をご覧ください。

Distributed Cloud DDoS Mitigation

ビジネス妨害を狙った標的型サービス拒否攻撃からネットワークとアプリケーションを保護するための効果的なセキュリティ

F5 Distributed Cloud DDoS Mitigation は、レイヤー 3、4、7 のインターネットプロトコルを標的とした、さまざまな DDoS 攻撃に対する防御を提供します。このサービスでは、以下のような一般的な DDoS 攻撃が緩和されます。

リフレクションおよびアンプフラッド攻撃	DNS キャッシュポイズニング
データグラムフラグメント化攻撃	脆弱性攻撃
TCP スタック攻撃	リソース枯渇攻撃
アプリケーション攻撃	フラッシュクラウド
SSL/TLS 攻撃	NXDOMAIN 攻撃

F5 Distributed Cloud Mitigation は、お客様のトラフィックを検査し、大規模なボリューム型 DDoS 攻撃のトラフィックをスクラブして、クリーントラフィックのみを通過させ、お客様のオリジンネットワークに安全に戻します。

DDoS Mitigation サービスに含まれる、自動適用されるエッジ攻撃緩和機能は、当社のネットワーク全体におけるすべてのお客様の既知の攻撃ベクトルのトラフィックを検知し、プロアクティブにブロックします。F5 SOC の DDoS エンジニアは、自動によるエッジ攻撃緩和機能では対処できない攻撃ベクトルを緩和するために、さらに詳細なトラフィック分析を行い、対策を講じます。F5 Distributed Cloud DDoS Mitigation は、DDoS 脅威の完全な可視化、レポートおよび脅威インテリジェンスサービスを提供し、既知の悪意のある脅威をブロックします。

お客様は、エッジネットワークデバイスやアプリケーションインフラストラクチャへの負担を回避するために、SOC のエンジニアと協力して、リターントラフィックのレート制限の値を設定できます。きめ細かい検知と攻撃緩和のメカニズムにより、ユーザー体験に影響を与えることなく、L7 DDoS 攻撃を柔軟に緩和できます。

F5 Distributed Cloud DDoS Mitigation マネージドサービスの構成要素

お客様は、F5 と協力して、DDoS アクティビティに対する最大の防御を実現し、最も悪質な攻撃を自動的に緩和できます。

運用モデル

F5 Distributed Cloud DDoS Mitigation マネージドサービスは、**Always On**（お客様のトラフィックが継続的に F5 ネットワークを通じてルーティングされます）または **Always Available**（F5 の SOC またはお客様が DDoS 攻撃の前または最中に F5 ネットワークへのルート変更を発動します）の 2 つの導入モードで提供されています。

統計が示すように、企業には DDOS 攻撃の標的にされるリスクがあります。これらの攻撃は、アプリケーションのパフォーマンスや可用性を妨害することを目的し、利用可能な帯域幅、CPU やメモリーなどのアプリケーションリソース、DNS や TLS などの重要なインフラストラクチャプロトコルなどを狙い、その攻撃ベクトルはさまざまです。

F5 Distributed Cloud DDoS Mitigation サービスは、1 年、2 年または 3 年の契約でご利用可能です。サービスのコストは、保護する FQDN（完全修飾ドメイン）の数、保護するデータセンターとルーターの数、95 パーセンタイル測定値（クリーンな帯域幅のピーク消費量：bps）、NetFlow/sFlow データ用に監視するエッジルーター、運用モード（Always On または Always Available）などで異なります。

導入モード

F5 Distributed Cloud DDoS Mitigation サービスは、**ルーティングモード**と**プロキシモード**の 2 つの異なるモードで利用できます。

ルーティングモード

Distributed Cloud DDoS Mitigation が提供するルーティングモードは、パブリックにアドバタイズされるルーティングサブネット [クラス C：CIDR /24 プレフィックス] を少なくとも 1 つ使用しているお客様向けのサービスです。このサービスは、Border Gateway Protocol（BGP）を利用して、F5 キャリアを通じてルーティングプレフィックスをアドバタイズします。ルーティングプレフィックスが F5 のプラットフォームとグローバルネットワークを通じてアナウンスされると、お客様のプレフィックスに送信されるすべてのお客様のトラフィックは、検査と攻撃緩和のために F5 のグローバルスクラビングセンターに送られます。お客様は、SOC のエンジニアの支援を受けながら、ルートアドバタイズを制御できます。

お客様は、1 つまたは複数の GRE（Generic Tunnel Encapsulation）トンネル、L2 接続、Equinix Fabric やその他の接続プロバイダを介した F5 のグローバルネットワークとのプライベートピアリングなど、複数の設定オプションを選択し、クリーントラフィックをお客様のネットワークに戻すことができます。SOC は、お客様と協力して、選択されたスクラビングセンターからプライマリおよびバックアップのリターンパスを提供することで、お客様のネットワークに完全な冗長性を構築します。

ロードバランサーモード

Distributed Cloud DDoS Mitigation サービスが提供するロードバランサー（LB）モードは、パブリックにアドバタイズ可能なルーティングサブネット [クラス C：CIDR /24 またはより特定のプレフィックス] を使用していないお客様向けのサービスです。この導入モードを利用するには、F5 Distributed Cloud アプリケーションのロードバランサーを導入する必要があります。ロードバランサーモードのお客様は、権威 DNS 解決を利用して、検査と攻撃緩和のために

トラフィックをスクラビングセンターに転送できます。ルーティングモードには 10 台のロードバランサーが含まれていますが、ルーティングモード導入とは別に、スタンドアロン構成のロードバランサーを購入することもできます。

プラットフォーム

F5 Distributed Cloud DDoS Mitigation マネージドサービスは、最大のレジリエンシ、優れた設定可能性、迅速な拡張性を求めて設計されたグローバルなソフトウェア定義ネットワーク（SDN）を採用しています。このネットワークは、22 のメトロリージョンに 24 のリージョナルエッジ（RE）があり、攻撃緩和に 13 Tbps の容量を利用できます。リージョナルエッジの位置は以下のとおりです。

F5 のサービス拒否攻撃防御は、お客様が望む実践管理レベルで、お客様のアプリケーションがホストされる場所（クラウド、オンプレミス、またはその両方）に基づき、ビジネスに最適なアーキテクチャと運用モデルで提供されます。

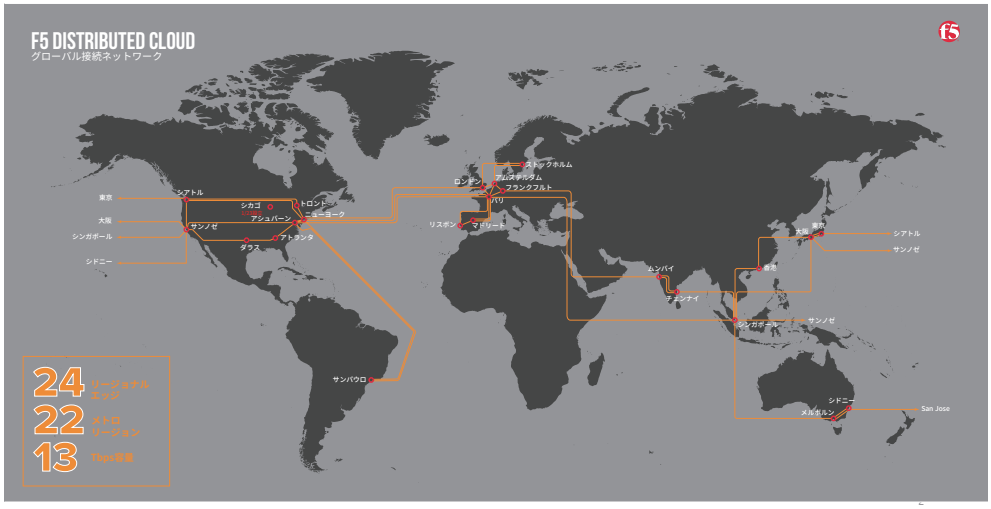


図 1：F5 Distributed Cloud のネットワーク

エッジでの自動攻撃緩和

このプラットフォームは、自動攻撃緩和によるエッジ保護を通じて、即座に攻撃緩和を提供します。ネットワークエッジでのアーキテクチャを強化するこのソリューションの基本的な強みは、最も一般的な攻撃ベクトルに対して非常に迅速な Time To Mitigate（TTM）を実現することです。DDoS 攻撃は、1 秒あたり膨大な量のパケットを送り込む帯域幅攻撃により数分程度でも特に大きな被害をもたらします。これらの攻撃は、保護されていない企業にとって壊滅的な打撃を与える可能性があります。この強化に関連する AI/ML テレメトリには、信じられないほど高速かつ効果的な速度で悪意のある攻撃トラフィックをブロックする能力があります。

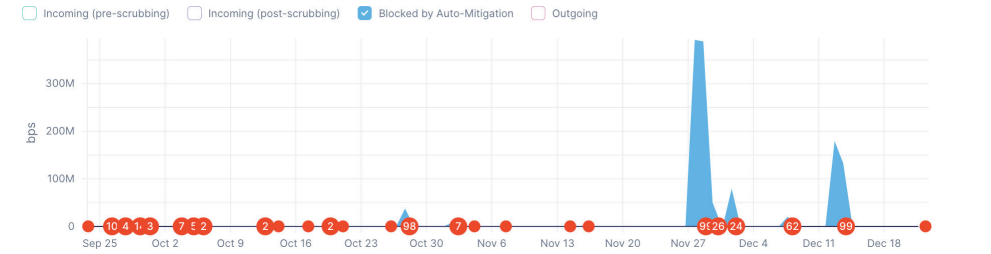


図 2：自動エッジ攻撃緩和

可視化

F5 Distributed Cloud DDoS Mitigation では、設定と可視化のための管理コンソールにアクセスできます。このコンソールは、DDoS 攻撃アクティビティに関する詳細なリアルタイム情報を提供します。

F5 のアプリケーションサービスは、従量課金、永久ライセンス、サブスクリプションおよびエンタープライズライセンス契約でご利用可能です。

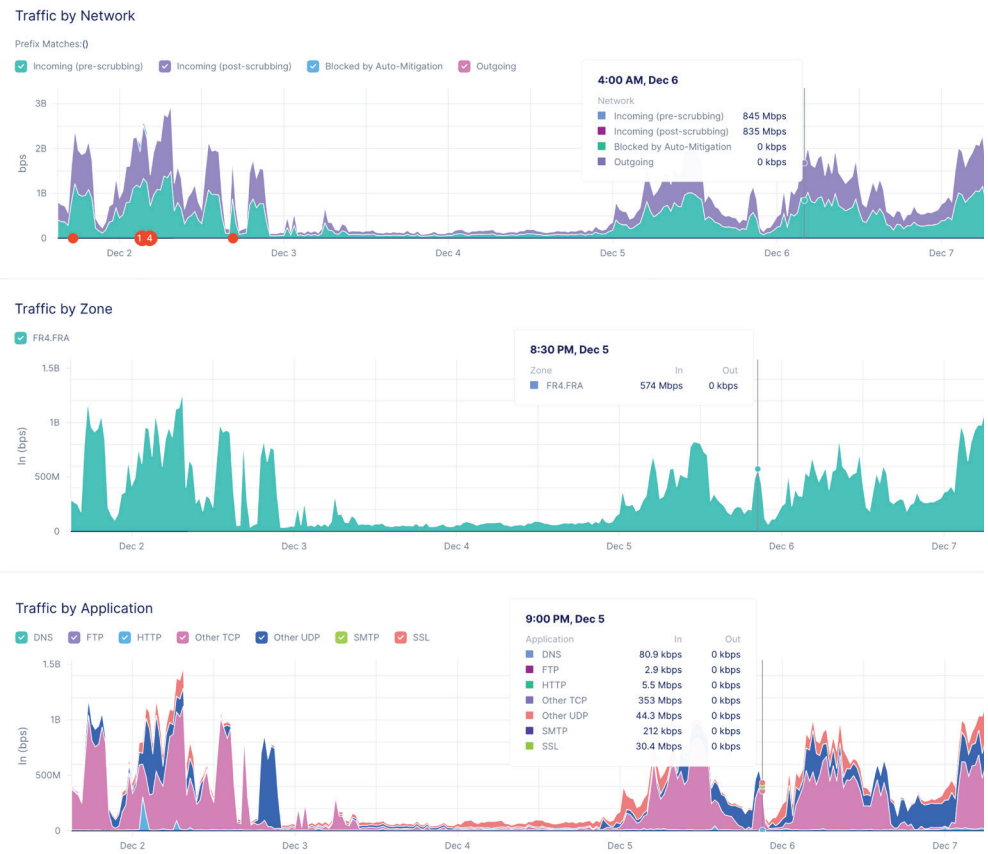


図 3：システム管理コンソールのトラフィックと攻撃緩和

- **攻撃の種類と規模**
- **攻撃起点**
- **攻撃緩和技術**
- **攻撃抑制に適用された対策**
- **攻撃に使用されたプロトコル**
- **攻撃された IP アドレスの範囲とポート**
- **お客様ネットワークに対するインバウンドの攻撃トラフィックとアウトバウンドのクリーントラフィック**
- **DDoS 攻撃に関する日次レポート**

このコンソールでは、特定期間の DDoS 攻撃パターンに関する情報や、ユーザーペルソナに基づいた関連情報を表示するカスタマイズ可能な DDoS ダッシュボードも提供されます。さらに、オンデマンドで定期的なレポートも利用できます。

主な特徴

マルチレイヤーのグローバル DDoS 防御
DDoS 攻撃緩和ツールと技術は、F5 Distributed Cloud のグローバルネットワークのエッジ全体に分散し、大規模なボリューム型攻撃に対する防御を提供します。エッジに適用される攻撃緩和対策は、L3/L4 プロトコルの脅威や高度な L7 アプリケーションの DoS 攻撃を防ぎます。

大容量防御
F5 Distributed Cloud のセキュアなグローバルネットワークとスクラビングインフラストラクチャは、世界中 23 のネットワークエッジに広がり、13Tbps 以上の容量で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。

柔軟でスケーラブルなサービスオプション
F5 は、さまざまな規模の攻撃を緩和でき、お客様のネットワークやアプリケーション構成の保護に特化したカスタムビルドのソリューションを提供するためのサービスセレクションを提供しています。このサービスは、BGP またはロードバランサーのルーティングを On-Demand または Always-On のサービスオプションで提供します。

可観測性と管理の一元化
F5 Distributed Cloud コンソールは、DDoS 攻撃アクティビティに関する実用的な情報を、単一の管理インターフェイスで提供します。

専門家による管理と攻撃緩和
継続的な攻撃の監視 / 攻撃緩和を行い、業界をリードする F5 SOC のエンジニアチームを活用して、お客様のすべてのアプリケーションの最高レベルの保護とアップタイムを実現します。

NetOps/DevOps/SOCOps 統合 API

F5 Distributed Cloud プラットフォームは API ファーストの SaaS 型サービスであり、すべてのシステム機能は REST API を介して公開され、API Dev ポータルで文書化されています。現在開発中の API によるシステム機能拡張では、API コールにより、ルートアナウンスの有効化 / 無効化、新しいプレフィックスの定義、トンネルの構築、追加のレポートメトリクスの取得、その他の機能が可能になる予定です。

システムステータス

F5 Distributed Cloud サービスのリアルタイムなシステムステータスは、外部でホストされるポータルサイトで確認できます。F5 Distributed Cloud は、通常保守作業について遅くても 15 暦日前までに通知します。しかし、F5 は緊急保守をいつでも実施する権利を有します。緊急保守については、保守作業の実施前に通知されます。現在および過去の保守に関する通知は、カスタマーポータルおよび F5 Distributed Cloud Status から確認できます。ステータス更新を利用することで、リアルタイムの通知をお好みの通信方法で受け取ることができます。

攻撃緩和ワークフロー

DDoS アナリストは、さまざまなツールセットを通じてお客様のプレフィックスを継続的に監視します。悪意のあるアクティビティを検知した場合、以下のことが行われます。

1. F5 の攻撃緩和ギアにより攻撃（ツールセットからのアラート / イベント / ベースライン / しきい値）として分類される可能性のある状態が差し迫っていることが、SOC のエンジニアに通知されます。
2. 複数の SOC のアナリストが、適切な攻撃緩和措置を講じるための手順を開始します。
3. SOC のプライマリエンジニアが、観測されたベクトルに基づいた攻撃緩和パラメータの構築を開始し、可能な限り詳細かつ効果のある対策を講じるとともに、F5 のスクラビングセンターを通過するルートがルートリークのない最適なルートであることを確認します。
4. SOC のセカンダリチームが、お客様のコンソールテナントに記載されているリアルタイムインシデント対応手順（RTIP）を確認し、それに従って行動します。これらの手順の一環として、お客様の SOC/NOC/DevOps/NetOps 管理者に電話連絡する、または継続的な解決追跡を目的としてお客様のチームに送信するエスカレーションインシデントを生成することがあります。
5. 攻撃アクティビティが緩和された後、お客様は SOC チームにポストインシデントレポートを要求できます。

顧客事例

F5 Distributed Cloud DDoS Mitigation サービスでは、契約期間中、カスタマーサクセスマネージャ（CSM）が任命され、お客様のアカウントに割り当てられます。CSM は、オンボーディングプロセスにおいてお客様と協力して、すべてのタスクを正常に完了します。CSM は、オンボーディング完了後も引き続きお客様と協力して、適切なスケジュール（通常は四半期または半年ごと）の定期チェックポイントを設け、お客様の設定、システム利用、業界動向、サービスの新機能や強化を確認するため、および将来の成長や追加サービスの取得を計画するための支援を行います。

F5 は、大規模なボリューム型 DDoS や標的型アプリケーション DoS からリアルタイムに保護する DDoS 攻撃緩和サービスを提供し、混合型の高度なマルチベクトル攻撃からお客様のビジネスを守ります。

追加サービス

F5 Distributed Cloud DDoS Mitigation は、お客様が保護と脅威軽減を強化するために活用できる追加の補完サービスを提供します。

脅威インテリジェンス

脅威インテリジェンスは、Always On および Always Available をご利用のお客様向けのアドオンサービスです。このサービスを利用するには、アプリケーションプロキシを導入する必要があります。脅威インテリジェンスは、IP レピュテーションを活用してトラフィックをブロックし、継続的に更新される既知の不正 IP アドレスリストを使用します。お客様は、特定された悪意のあるアクターのサブカテゴリーを選択し、それらのアクティビティがお客様のオリジンネットワークやアプリケーションに到達しないようにブロックできます。

ルーターの監視

ルーターの NetFlow または sFlow 監視は、Always Available のお客様向けのアドオンサービスです。ルーター監視サービスは、お客様のエッジルーターのトラフィックサンプルを利用して、ボリューム型の L3/L4/L7 DDoS 攻撃に関連する潜在的なアクティビティを検知します。F5 SOC は継続的にデータを分析し、DDoS 攻撃を検知した場合にはお客様にアラートを通知します。SOC は、お客様と協力して、攻撃に対応するための内部ポリシーを定義し、自動的またはお客様のご要望に応じて、攻撃緩和のためにお客様のトラフィックをスクラビングセンターにリダイレクトします。

サービス提供責任

タスク	お客様	F5 DISTRIBUTED CLOUD SOC
クリーントラフィック配信の設定	お客様は SOC と協力して GRE トンネル / プライベートリンクを構築します。	SOC エンジニアは GRE トンネル / プライベートリンクをプロビジョニングします。
ロードバランサーの設定	お客様はロードバランサーを導入するか、SOC エンジニアと協力してカスタマーコンソールを使ってロードバランサーをプロビジョニングします。	SOCのエンジニアは、お客様のご要望に応じてロードバランサーの構築をサポートします。
ルーター監視の設定	お客様はエッジルーターのフロー設定情報を提供します。	SOC のエンジニアは、お客様のルーターからフロー情報を受信できるようにサービスを設定します。
エッジ攻撃緩和ルールの設定	お客様は SOC と協力してエッジ攻撃緩和ルールを定義します。	SOC のエンジニアはルールを構築および設定します。
脅威インテリジェンスの設定	お客様は SOC と協力して、脅威インテリジェンスのルールを設定します。	SOC のエンジニアは脅威インテリジェンスのプロファイルを構築します。
DDoS 攻撃検知	SOC エンジニアリングチームにより自動的に導入および実施されます。SOC による攻撃緩和実行の手順については、「移行ワークフロー」をご覧ください。	SOC のエンジニアは、トラフィックの異常を検査し、攻撃を確認して、エッジ攻撃緩和で特定できなかった攻撃を緩和するための対策を適用します。
F5 Distributed Cloud でのトラフィックルート	お客様は、ルーティングモードの場合は BGP を介して、あるいはプロキシモードの場合は DNS 解決を介して、トラフィックを F5 Distributed Cloud プラットフォームにルーティングします。	必要に応じて SOC の支援を受けることができます。
L3/L4/L7プロトコルにおけるボリューム型 DDoS 攻撃の緩和	お客様による対応は不要です。攻撃中、お客様は SOC と協力して、同時対策やトラフィックシェーピングを行うことができます。	SOC のエンジニアは、攻撃の種類に応じて適切な攻撃緩和を導入します。
L7 プロトコルの DDoS 防御	お客様は SOC と協力して、L7 攻撃ベクトルに対するしきい値を定義します。	SOC のエンジニアは、お客様のご要望に応じて、しきい値と攻撃緩和設定に関する推奨事項を提供します。

サービス品質保証	サービス品質の説明	補償
99.99% のアップタイム	攻撃を緩和するための Distributed Cloud DDoS Protection サービスの 99.99% の可用性	お客様は、サービス停止の期間に基づいて、以下の表で定義されるサービスクレジットを受けることができます。 サービス停止期間　サービスクレジット > 連続 60 秒以上　2 日 > 連続 60 分以上　5 日 > 連続 24 時間以上　10 日
Time to Notify（TTN）：15 分	F5 がお客様に攻撃インシデントの発生を通知するまでに許容される最大時間	お客様は、1 回の違反につき 1 日のサービスクレジットを受けることができます。
Time to Mitigate（TTM）：15 分	F5 が DDoS 攻撃緩和を開始するまでに許容される最大時間（エッジ攻撃緩和は秒単位で自動的に発生します）	お客様は、1 回の違反につき 1 日のサービスクレジットを受けることができます。
サポートエスカレーション	攻撃インシデントは、15 分以内に Tier-2 および Tier-3 サポートにエスカレーションされます。	お客様は、1 回の違反につき 1 日のサービスクレジットを受けることができます。

DC 01.2023 | JOB-CODE-123456789