CUSTOMER PREPARATION GUIDE

F5® Distributed Cloud WAF
Managed Service Onboarding

本書は、お客様のネットワークエンジニアリング、NOC/SOCおよびアプリケーション開発チームが、F5 Distributed Cloud WAFサービスに迅速にオンボーディングできるように準備するための技術ガイドです。

標準および緊急導入対応

OWASP アプリケーション セキュリティ
アプリケーションレイヤー攻撃からアプリケーションを保護して、それぞれの独自のポリシーをカスタマイズできます。

簡単な導入
F5 のセキュリティ専門家によるサポートを受けながらアプリケーションをオンボーディングすることで、保護までの時間を短縮します。ハードウェアやソフトウェアの導入も管理も不要です。

SaaS 型、グローバルに利用可能、ビジネスへの影響なし
F5 グローバルネットワークおよび SOC のアナリストを活用して、継続的なアプリケーション可用性を保持できます。

手頃な価格の参入および所有コスト
SaaS 型のマネージドサービス F5 Distributed Cloud Services を 利用することで、必要なサービスを手頃な価格で取得して、総所有コストを最適化できます。

F5 Distributed Cloud Serviceは、SaaS型のセキュリティ、ネットワーキングおよびアプリケーション管理サービスであり、データセンター、マルチクラウド、エンタープライズエッジなど、必要な場所にクラウドネイティブ環境でアプリケーションを導入、保護、運用することを可能にします。

サービスには、お客様のセキュリティおよびインフラストラクチャ要件に合うさまざまなソリューションが含まれます。お客様は、クラウドとエッジのサイト管理、コンテンツ配信および DNS 管理、ロードバランサー、WAF、API 保護などを活用できます。

このガイドでは、主に *WAF（Web Application Firewall）* サービスに焦点を当て、特に、お客様がアプリケーションをプラットフォーム上にオンボードし、即時かつ最大の検知および攻撃緩和能力を得るために実行する必要のあるプロセスについて説明します。

WAF アプリケーション保護

F5 のネットワークと WAF 攻撃緩和のアーキテクチャは、広範囲なグローバル展開、他のキャリアのネットワークとの優れたピアリング、トラフィックをオリジンに戻すプライベートルーティングを可能にする直接接続オプション、エッジでの自動攻撃緩和を提供します。これには以下が含まれます。

- スケーラブルな設計
- 柔軟な接続オプション
- プライベートピアリング
- 最新のサービスプロバイダ向けグローバルバックボーン
- トップ 10 の IPv4 および IPv6 グローバルピアリングネットワーク
- 24/7 体制のグローバルセキュリティオペレーションセンター

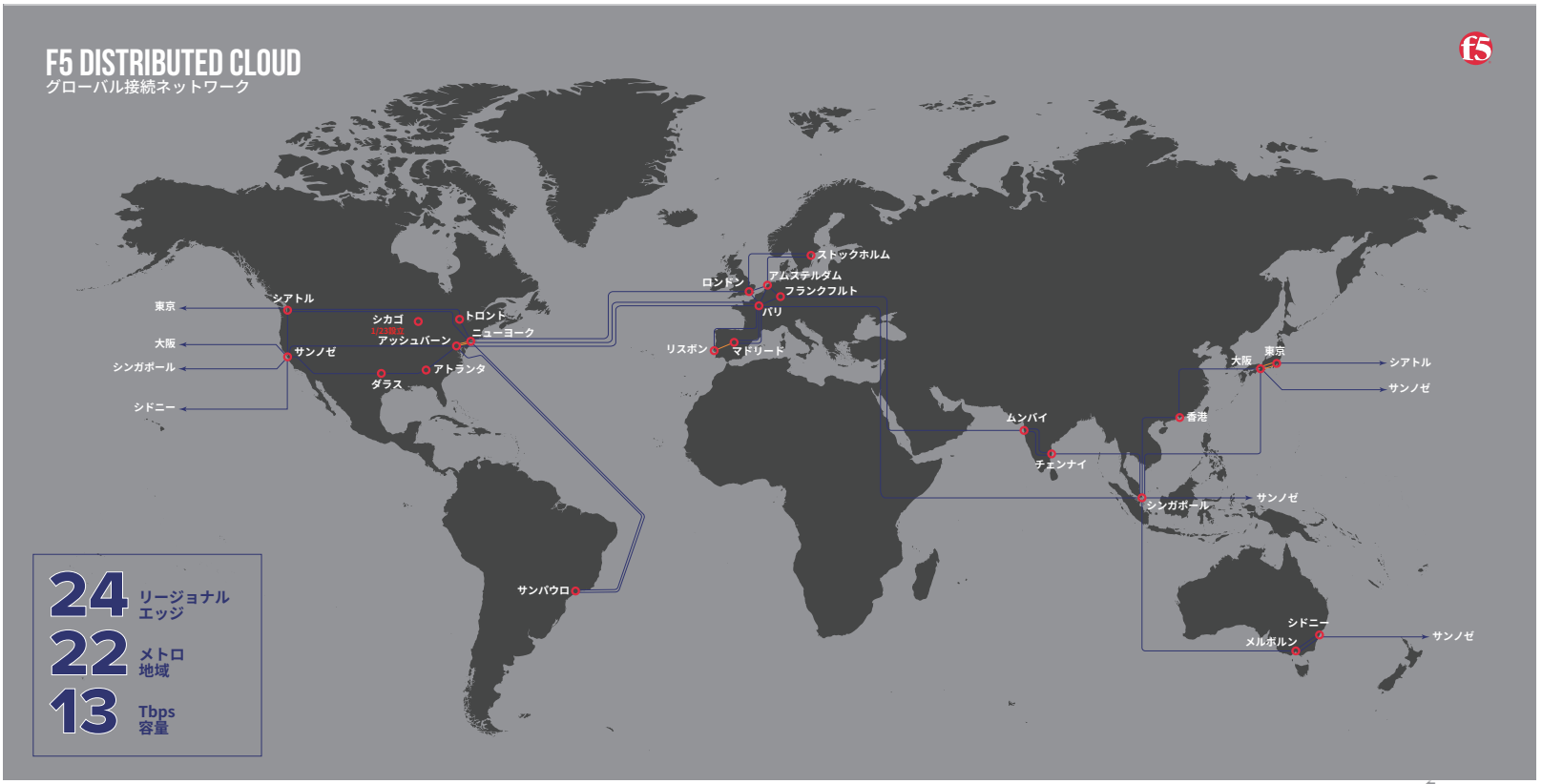

図 1：F5 Distributed Cloud グローバルネットワーク

WAF の脆弱性

アプリケーションを狙った攻撃は、さまざまな形で発生し、脆弱性として知られる非常に特殊な攻撃ベクトルを標的とします。脆弱性の種類は、以下のように分類できます。

OWASP Top Ten（下表参照）
Common Vulnerabilities and Exposures（CVE）
ゼロデイ攻撃の脆弱性

アクセス制御の不備	脆弱や古くなったコンポーネント
暗号化の失敗	識別と認証の失敗
インジェクション	ソフトウェアとデータの整合性の不具合
安全が確認されない不安な設計	セキュリティログとモニタリングの失敗
セキュリティの設定ミス	サーバーサイドリクエストフォージェリ

OWASP TOP TEN

表 1：OWASP Top Ten：WAF の脆弱性

Top Ten は、OWASP という組織により Web アプリケーションにおける最も重大なセキュリティリスクとして特定されている脆弱性です。

その他、CVE(Common Vulnerabilities and Exposures) をターゲットにした攻撃もあります。これらは、インフラストラクチャとアプリケーションコードのフレームワークの両方における実際に**悪用が確認**されたものです。F5 Distributed Cloud WAF のポリシーは、お客様が使用および公開するアプリケーションの範囲全体を保護するようにカスタマイズできます。F5 Distributed Cloud WAF のポリシーは、お客様が使用および公開するアプリケーションの範囲全体を保護するようにカスタマイズできます。

第 3 の攻撃カテゴリーは、アプリケーションコード内の未知の脆弱性を悪用して発展する攻撃です。この種の攻撃は非常に悪質であり、迅速に解決しなければ、被害者のアプリケーションに深刻な損害を与える可能性があります。これらは、ゼロデイ攻撃として知られています。最近確認されたゼロデイ脆弱性は、Apache Log4j のエクスプロイトです。

お客様は、F5 Distributed Cloud のセキュリティエンジニアと協力して、脆弱性を特定し、それらの脆弱性を狙う特定の攻撃をブロックする WAF ポリシーを構築できます。アプリケーションのフレームワークによって、脆弱性のセットは異なる可能性があるので注意してください。そのため、各アプリケーションフレームワークには、そのフレームワークに関連する脆弱性から保護するための特定のポリシーが構築されていることが非常に重要です。

また、サードパーティの脆弱性スキャナを使用して、定期的にアプリケーションを検査することをお勧めします。脆弱性スキャナで生成されるデータは、DevOps/NOC/SOC チームや F5 Distributed Cloud セキュリティエンジニアリングなどの内部顧客に提供して、アプリケーションのセキュリティ体制を強化し、将来のリリースの品質管理を確実にできます。

2022 年版アプリケーション戦略の状況レポートはこちらからダウンロードしてご覧ください

WAF Mitigation のアーキテクチャ

F5 Distributed Cloud は、24/7 体制のセキュリティオペレーションセンター（SOC）のエンジニアなど、マネージドオンボーディングのサポートと継続的なサポートにより支えられる強力な WAF エンジンを提供します。

WAF ポリシーは、柔軟な設計が可能であり、セキュリティスタンスに応じたさまざまな展開方法を選択できます。迅速に保護できるようにアプリケーションをすぐに導入することも、F5 SOC やエンジニアリングチームと連携して、アプリケーションの起動前にカスタムポリシーを開発することもできます。

ポリシーがブロッキングモードになると、お客様はトラフィックと攻撃の監視を続けることができます。アプリケーションへの機能の追加または変更がある場合、お客様は SOC チームと協力して、保護範囲をさらに強化できます。

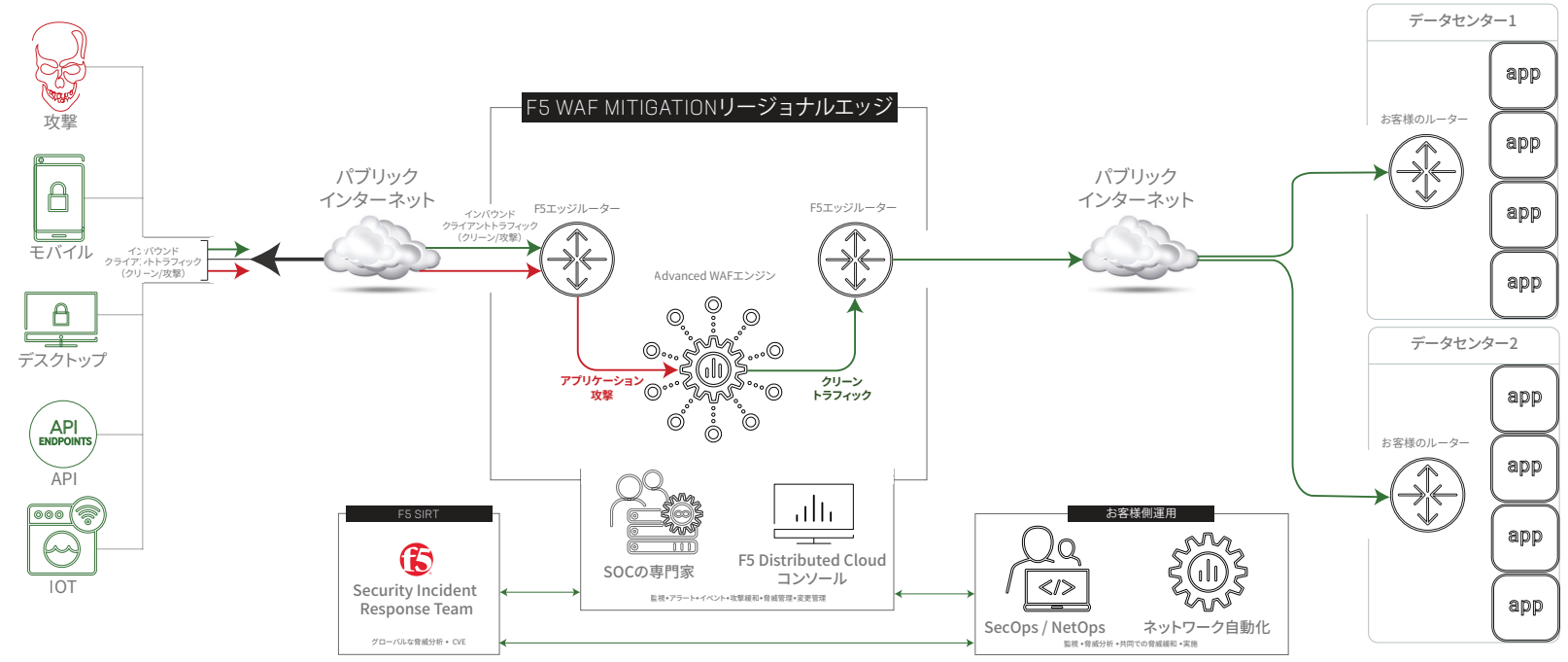

Figure 2 - WAF Protection and Mitigation Service

トラフィックのルーティング

お客様は、F5 Distributed Cloud プラットフォームの CNAME レコード、またはリージョナルエッジのロードバランサーがアクティブ化されたときに提供された IP アドレスに対して DNS の権威レコードと再帰レコードを指定することで、クライアントトラフィックをルーティングします。お客様は、F5 Distributed Cloud のステータスページにアクセスし、WAF 管理コンソールにログインすることで、お客様のアプリケーションとリージョナルエッジの状態を監視できます。

オンボーディングの準備

最初のミーティングの前

WAF Mitigation サービスの導入を成功させるために、お客様の技術チームは、F5 Distributed Cloud オンボーディングチームとのミーティング前に、リソースと正確な技術データを準備する必要があります。

WAF の概念

SOC との WAF の管理に積極的に関与するお客様のチームメンバーは、次のことを十分理解している必要があります。

F5 Distributed Cloud WAF（入門編）
F5 Distributed Cloud WAF（技術編）
WAF
HTTP
HTTPS
TLS
リージョナルエッジ
F5 HTTP ロードバランサー

お客様によるオンボードの準備
お客様は、要求されたすべての必要なデータを揃え、オンボーディングチームに渡す準備を整えておく必要があります。最初のオンボーディングミーティングでデータが揃ってない場合、ソリューションの導入が遅れる可能性があります。

現在攻撃を受けているお客様
ボリューム型 DDoS 攻撃を受けているお客様は、特別な配慮が必要な場合があります。攻撃を受けている状況では、緊急性プロビジョニングが必要になります。

リソースの準備
お客様は、適切なスタッフをプロジェクトに割り当てる必要があります。F5 Distributed Cloud オンボーディングチームは、専任のネットワークエンジニアとお客様の NOC/SOC チームの支援があることを理想としています。

リソースの制約
お客様は、F5 Distributed Cloud オンボーディングチームと協力して、人員やリソースに関する潜在的な制約を特定する必要があります。

お客様 データ

Distributed Cloud WAF サービスを最も円滑かつ迅速に導入するために、お客様の技術チームは、F5 Distributed Cloud オンボーディングチームとの最初のミーティングに**先立ち**、以下の情報を入手しておく必要があります。

重要 **最初のミーティングまでにお客様の設定データがオンボーディングチームに提供されていない場合、オンボーディングの完了が遅れる可能性があります。**

保護するアプリケーション

お客様は、保護範囲内に含める予定のすべてのアプリケーションの完全なリストおよび明記した目的を提供する必要があります（FQDN、ポート、ルーティング）。

ポリシーの開発 / 実施

お客様は、ポリシーの開発と実施について、2つのモードから選択できます。

モニタリングモード： DevOpsチームは、F5 SOCのエンジニアと協力して、段階的にポリシーを開発およびテストできます。このモードでは、モニタリング（学習）モードからポリシーを開始します。お客様とSOCチームは協力して、特定されたWAF違反を確認し、特定の攻撃タイプに対処するためにポリシーを修正します。ポリシーの修正が完了したら、お客様はSOCに対して、ポリシーの状態をブロッキングモードに修正するよう依頼できます。

ブロッキングモード： このモードでは、ポリシーをモニタリングモードにせずに、直ちにブロッキングモードにします。このモードは、すでにアプリケーションを運用しているお客様が、現在攻撃を受けている、または差し迫った攻撃の脅威にさらされている場合にお勧めします。

ブロッキングレスポンスページ

お客様は、ポリシーによってHTTPリクエストがブロックされたときに発行したいレスポンスを定義するHTMLコードをオンボーディングチームに提供する準備をしておく必要があります。このページは、すべてのWebアプリケーションファイアウォールポリシーで有効にする必要があります。また、このページは、ブロックされたリクエストの電子メールアドレスまたは電話番号を提供する必要があります。

アプリケーションのフレームワーク

お客様は、アプリケーションの開発と運用をサポートするために採用したすべてのフレームワークとコンポーネントを特定する必要があります。

SNI/SAN

お客様のチームは、アプリケーションルーティングにSNI とSAN のどちらを使用する予定であるかを特定する必要があります。

TLS セキュリティ / 相互 TLS

お客様は、独自のドメイン証明書を使用するか、またはF5 Distributed CloudサービスによってプロビジョニングされるletsEncrypt証明書を導入するかを指定する必要があります。LetsEncryptは、信頼の鎖の中でエンドエンティティ証明書として機能します。

アプリケーションのオリジン IP/CNAME

お客様のチームは、すべてのクリーントラフィックをオリジンロードバランサーまたはアプリケーションサーバー/フレームワーク（お客様のデータセンター）に返すためのリターンパスを特定する必要があります。また、WAF保護以外の目的で使用されているプロキシがあれば、インラインですべてリストしてください。

シグネチャベースのボット対策

お客様は、3つのカテゴリーのシグネチャベースのボット対策をドメイン上で有効にする場合：**悪意のボット/疑わしいボット/善意のボット**と、アクション：**ブロックまたは報告**を選択できます。

シグネチャベースのボット対策

許可/拒否リスト用のIPアドレスを提供してください。

プロビジョニングと追加システム要件の検討

HTTP ロードバランサー

1. 新しいロードバランサーの作成
2. メタデータ、ドメイン、LB タイプの設定
3. オリジンプールの設定
4. ルートの設定
5. セキュリティ構成の設定
6. その他の設定
7. LB のプロビジョニングの完了
8. LB 状態の確認

WAF

1. 新しい WAF オブジェクトの作成
2. メタデータと WAF モードの設定
3. 検出構成の設定
4. シグネチャボット保護の設定
5. レスポンス構成の設定
6. WAF オブジェクトのプロビジョニングの完了

WAF 設定 API

アプリケーションファイアウォールの作成　メトリクス　アプリケーションファイアウォールの取得
アプリケーションファイアウォールの交換　アプリケーションファイアウォールのリスト　アプリケーションファイアウォールの削除

オンボーディングのワークフロー

サービスプロビジョニング ①

管理コンソール
契約パラメータ設定

- **管理コンソールのテナントアカウントのプロビジョニング**
  クラウドサポートチームが、コンソールでお客様アカウントを作成し、お客様のテナントを設定、サービス運用パラメータを定義、グローバル管理者ユーザーアカウントを設定します。お客様のテナントアカウントが有効になり、サービスのプロビジョニングの準備が整うと、電子メールで通知が送信されます。
- **追加テナントユーザーのアカウントの作成**
  お客様は、ご自身でコンソールにアクセスして、システムの追加ユーザー用のアカウントを作成し、保護サービスを操作するための適切なアクセス認証情報を付与するか、あるいはオンボーディングチームにこのタスクの完了を依頼できます。

サービス紹介 ②

最初のミーティング
オンボーディングチームとの最初のミーティングの設定

- **お客様との最初のミーティングのスケジュール**
  テナントが作成され、お客様が管理コンソールに正常にアクセスできることが確認されると、オンボーディングチームは、最初のプロジェクトレビューミーティングの案内をお客様のプロジェクトリーダーに送信します。お客様のプロジェクトリーダーは、プロジェクト関係者全員をこのミーティングに招待し、前セクションに記載されているすべての必要なデータをオンボーディングチームに渡せるように用意しておく必要があります。

サービス開始 ③

オンボーディングとCSM チーム
最初のミーティング：プロジェクトレビュー

- **オンボーディングチーム**
  最初のミーティングでは、オンボーディングチームは、プロジェクト完了に必要なすべてのステップの詳しい説明、ガイドラインとベストプラクティスの提供、ソリューション設計の支援、お客様が期待する結果の設定、WAFサービスに関する質問への回答を行います。オンボーディングチームは、プロビジョニングまでお客さまの必要なすべてのデータがミーティングで準備できていることを想定しています。
- **CSMチーム**
  完全なサービスパッケージの一部として、カスタマーサービスマネージャー（CSM）が任命されます。CSMは、カスタマージャーニーのすべてのステップに参加し、WAFサービスに関連するあらゆる項目のアドバイザーとして活動します。

サービス導入 ④

サービスコンポーネント
最初のオンボーディング設定

- **HTTPロードバランサー w WAFポリシー w 許容/拒否リスト w SSL w オリジン**
  オンボーディングチームは、データ収集段階とソリューション設計段階でお客様の要件によって定義された、すべての新しいHTTPロードバランサー、WAFポリシー、許可/拒否リスト、SSL証明書、オリジン宛先を作成します。お客様は、本番トラフィックを受信する前に、オンボーディングチームと協力して、コンポーネントが適切に設定されていることを確認します。
- **オンボーディング中の追加範囲設定**
  オンボーディングチームは、最初のプロビジョニング範囲の作業を行い、この段階で提供されたFQDNを設定します。最初の範囲を変更するには、実行前にオンボーディングチームによるレビューと承認が必要です。

P7に続く

オンボーディングのワークフロー （P6 からの続き）

サービスアクティベーション ⑤

本番トラフィック
FQDN DNS 権威解決

- **ロードバランサーへのライブトラフィックの指定**
  お客様は、クライアントトラフィックがF5 Distributed Cloudプラットフォームに送られるように各FQDNの権威ドメイン解決（DNS）レコードを変更する必要があります。本番環境にスムーズに移行できるように、オンボーディングチームと協力して、すべてのDNSレコードの変更を調整することをお勧めします。
- **品質保証：本番トラフィックの検証/完全性**
  DNSレコードの変更が有効になったら、トラフィックのフロー全体をテストすることをお勧めします。これらのテストでは、アプリケーションのすべての要素がお客様のクライアント（Webブラウザまたはその他のクライアント）に提供されていることを確認し、DNSの変更が構成される前と後でのアプリケーションパフォーマンスを測定する必要があります。

サービス移行 ⑥

セキュリティオペレーションセンター（SOC）
本番ベースのサポートと運用

- **オンボーディングチーム：お客様のSOCサポートへの移行**
  オンボーディングチームによる初期導入が完了すると、お客様はSOCによる継続的なサポートに移行されます。SOCは、新しいLBとポリシーの追加設定、既存のポリシーの調整、ロードバランサーの値の変更、およびお客様のセキュリティ体制のパフォーマンス分析と継続的な進化を支援します。
- **お客様管理コンソールの操作**
  お客様は、F5 Distributed Cloudの管理コンソールのすべてにアクセスできるので、WAFサービスのオンボーディングと継続的な運用の両方で説明される機能のほとんどを実行できます。お客様は、サービス上の任意のパラメータを変更できますが、本番環境に影響を与える変更は、SOCとCSMの両チームと調整することを強くお勧めします。
- **カスタマーサポートインシデント**
  お客様は、電子メール、管理コンソールまたは電話でサービスリクエストを開くことによって、SOCにサポートを申請できます。オンボーディングチームは、お客様がSOCチームに連絡するために使用できるさまざまな方法とエスカレーション手順のすべてを説明します。

サービス監視 ⑦

ネットワークとサービスの状態
F5 とお客様の運用

- **システムステータス**
  お客様のSOC/NOC/DevOpsは、このリンクを選択することにより、F5 Distributed Cloudサービスの状態を監視できます。F5ネットワークに影響を与えるあらゆる問題をお客様に通知できるように、このページは常に表示できるようにしておくことをお勧めします。
- **お客様管理コンソール**
  お客様は、コンソールにアクセスし、ロードバランサーの運用、WAFポリシー、積極的に攻撃緩和されたトラフィックに関連するさまざまなアクティビティのレポートを取得できます。オンボーディングチームは、オンボーディング/ポリシーの進化段階と本番環境での監視が重要となるさまざまなデータポイントを確認します。
- **お客様のナレッジベース**
  F5 Distributed Cloud サービスは、 その運用に関連するドキュメントの包括的なリポジトリを提供します。 プラットフォームについて理解できるように、 ナレッジベースを活用してください。

Distributed Cloud Services

1. 初期ポータルアカウントをプロビジョニング
2. オンボーディングチームがサービス導入を開始

F5 DISTRIBUTED CLOUD
アカウントの作成

オリジンプールの作成

1. 新しいオリジンプールを追加
2. 新しいオリジンプールに名前、ラベルおよび説明を設定
3. 1つまたは複数のオリジンサーバーを追加
4. 必要に応じてヘルスチェックを追加
5. オリジンプールのメンバーに接続するためのTLS設定を定義

アプリファイアウォールの作成、セキュリティポリシーの定義

1. 新しいアプリファイアウォールに
2. 名前、ラベルおよび説明を設定
3. 実施モードを選択
4. 検出設定とボット保護設定を選択
5. I必要に応じて、許可されたレスポンスコード、ログ内の機密性の高い値のマスキング、およびカスタムレスポンスページの使用を選択
6. 設定を保存および適用

DNSの委任

1. ロードバランサー/WAFコンポーネントのある、ホストされたエンドポイントに対して、F5 Distributed Cloudがトラフィックをルーティングするには、DNS委任が必要です。
2. まず、HTTPロードバランサーエンドポイントのDNSエイリアスを取得する必要があります。
3. 次に、DNSプロバイダのコンソールで自分自身のドメインのDNSレコードを更新する必要があります。この方法については、プロバイダの説明書をご覧ください。
4. 次に、一般的なDNSルックアップツールを使用して、エイリアス更新が適用されたことを確認できます。

HTTPロードバランサーの作成

1. 新しいHTTPロードバランサーを追加
2. 新しいHTTPロードバランサーに名前、ラベルおよび説明を設定
3. ロードバランサーに追加したドメインがトラフィックを渡す
4. TLS（HTTPS）設定を定義（ここでは自動的にプロビジョニングされた証明書を使用）
5. 使用するオリジンプールを定義
6. ロードバランサーのVIPをアドバタイズする場所を選択
7. Web Application Firewall設定を選択
8. 設定を保存および
9. 適用 DNSと証明書プロビジョニング

アクセス制御の決定

1. アプリケーションがF5グローバルネットワーク外にある場合、クライアントからトラフィックを直接受信できないようにアプリケーションを設定する必要があります。これにより、すべてのリクエストはWAFを経由してルーティングされ、それに応じて分析、処理、実行されるようになります。

検証品質保証

1. **トラフィックがWAFエンドポイントを通過**

   YWAFが設置されていて、トラフィックが許可または拒否されていることを検証するには、以下の手順を実行します。

   curl -v https:{your domain name}/uri

   セキュリティ監視ダッシュボードを確認

2. 少々の時間を取って、コンソールで利用できるダッシュボードとレポートの理解を深めてください。

   お勧めのダッシュボードとレポート：

   Malicious Users（悪意のあるユーザー）ダッシュボード
   Security Events（セキュリティイベント）ダッシュボード
   DDoSダッシュボード

Web Application Firewall

オンボーディングシナリオ1

参考資料

OWASP (Open Web Application Security Project)

OWASP WAFベストプラクティスガイド

応用アプリケーションセキュリティ：ポジティブセキュリティとネガティブセキュリティの効率性

Web Application Firewallとは

DC0420 | JOB-CODE-123456789