



2024/3

F5 Distributed Cloud WAAP Security Good practice Guide

F5ネットワークスジャパン合同会社

本資料の注意点

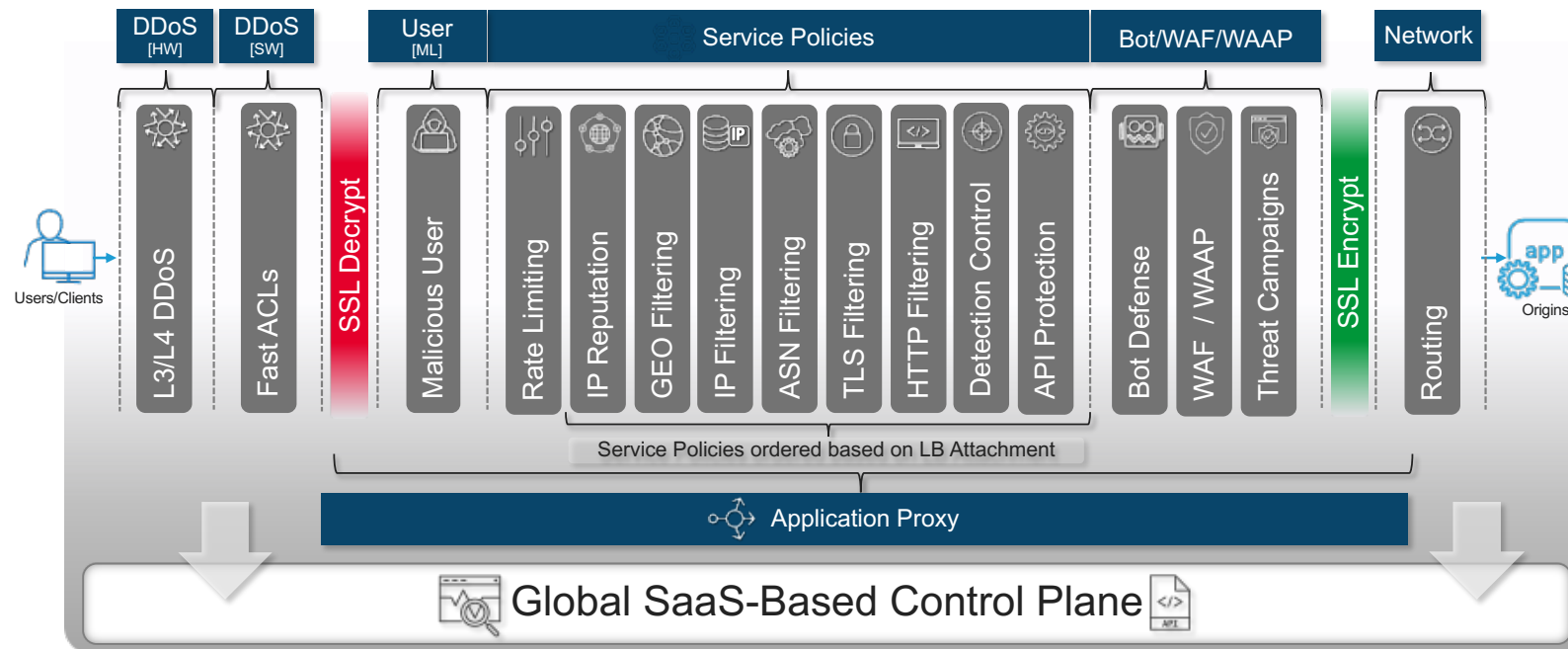
- 本資料は、資料作成時点のサービス内容およびライセンスについて記載しています。最新の情報は、F5 Distributed Cloud Servicesの[公式サイト](#)を参照ください。
- 技術的な内容に関するお問い合わせは、ご契約済みのお客様はサポート窓口、それ以外のお客様は当社営業/SE、または[問い合わせ窓口](#)までご連絡ください。

免責事項

このガイドに記載されている情報は、当社のプラットフォームでの実際のお客様の事例に基づいています。当社は、正確で信頼性の高い情報を提供するように努めていますが、この情報の有効性は時間の経過とともに変化する可能性があります。また、個々のお客様には個別要件があることから、この情報がすべてのお客様の環境に適していることを保証するものではありません。

1. F5XCの多層セキュリティ防御の理解

- F5XC Cloud WAAPは、多層防御の原則に従い、複数のセキュリティ機能を実装しています
- クライアントからのリクエストは、オリジンに到達する前に、これらのセキュリティ機構を通過します
- 各防御層により、お客様はさまざまなタイプの攻撃を適切に制御および防御できます
- お客様は、必要に応じて、ライセンスを購入ししこれらのサービスを有効にすることができます
- 各防御層により、お客様はさまざまなタイプの攻撃を適切に制御および防御できます

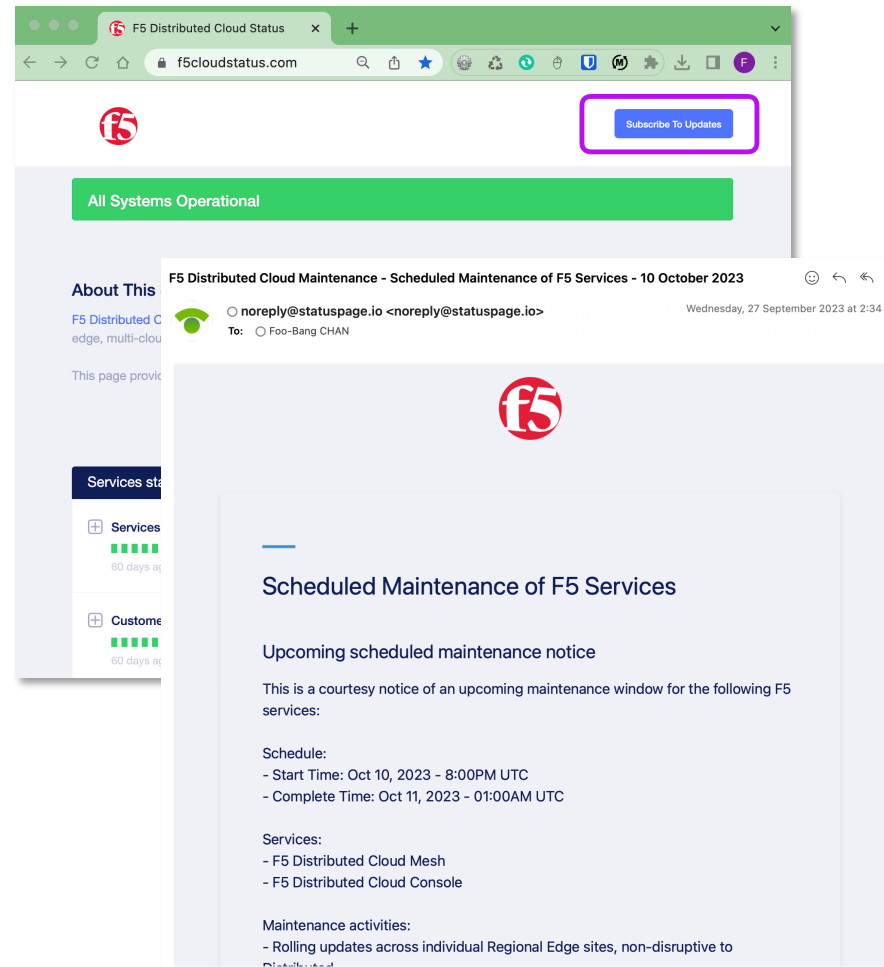


2. 重要な通知を受信するための F5 Cloud Statusのサブスクライブ設定

F5は定期的なスケジュールメンテナンスを実施します。メンテナンスに関する情報や、障害情報、また現在のサービスステータスなどは、以下のサイトで公開しています。

<https://www.f5cloudstatus.com>

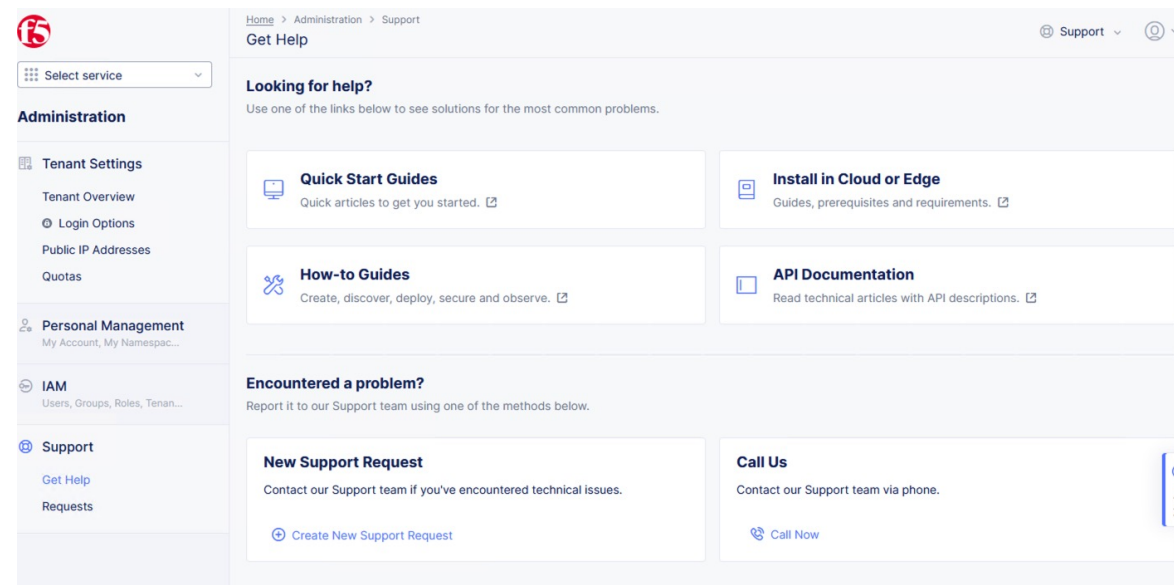
このサイトの“Subscribe To Update”より、Eメール、Webhook、Atom/RSSでのサブスクライブが可能です。いずれかの方法で通知を受信することを推奨します。



3. 問題が発生した場合のエスカレーション先の確認

F5 XC WAAPの標準サポートでは、
以下の3つの方法でサポートチケットを作成できます。
(英語での対応となります)

- F5 XC ポータルからのチケットの起票
- support@cloud.f5.com 宛のメール
- 電話



チケットの作成方法などは、以下のFAQを参照ください。

<https://f5cloud.zendesk.com/hc/en-us/articles/4405850494999>

<https://f5cloud.zendesk.com/hc/en-us/articles/11084950465943>

<https://f5cloud.zendesk.com/hc/en-us/articles/10170577267863>

4. アラート通知の有効化

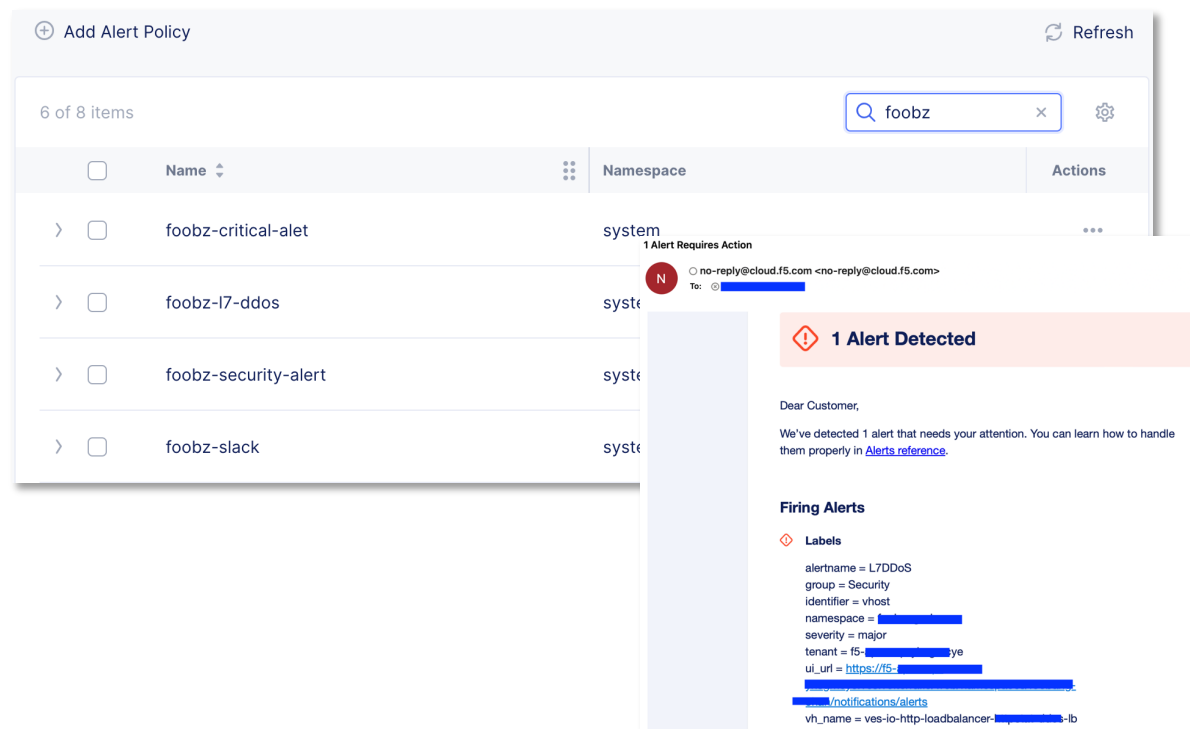
F5 XCでは、アラート通知をメール、SMS、Slack、PagerDuty、OpsGenie、Webhookで送信できます。

組織のアラート戦略はそれぞれ異なります。どのようなアラートが存在するか、F5XCアラートリファレンスを確認してください。

F5XCアラートリファレンスの詳細については、以下を参照ください。

<https://docs.cloud.f5.com/docs/reference/alert-ref>

利用しているサービスについて、Severitiesの“Critical”と“Major”のアラート通知を有効化することを推奨します。



5. Security EventsとRequest Logsを外部のSIEMに送信

F5XCでは、HTTP LBのアクセスログであるRequest LogsとWAAPの処理ログであるSecurity Eventsの保持期間があらかじめ設定されています。

Security Events – 30 日間

Request Logs – 7日間

Audit Logs – 30 日間

(DashboardのMetrics – 30 日間)

F5XCに保存されているログよりも長くログを保持するには、これらのログを外部のSIEMシステムに送信することを推奨します。

F5XCでは、Global Log Receiverを設定して、ログをSIEMに送信することが可能です。

Home > Shared Configuration > Manage
Global Log Receiver

+ Add Global Log Receiver [Tech Docs](#) Refresh

3 items Search

<input type="checkbox"/>	Name	Namespace	Actions
> <input type="checkbox"/>	foobz-global-log-stream	shared	...
> <input type="checkbox"/>	splunk-cloud-glr		
> <input type="checkbox"/>	splunk-ent-glr		

Global Log Receiver

* Log Type ⓘ

Request Logs ^

- Request Logs** Default
Send Request Logs (corresponding to Load Balancer access logs)
- Security Events**
Send Security Events (corresponding to e.g. WAF blocked events or malicious requests)
- Audit Logs**
Send Audit Logs (corresponding to Public Audit and Authentication)

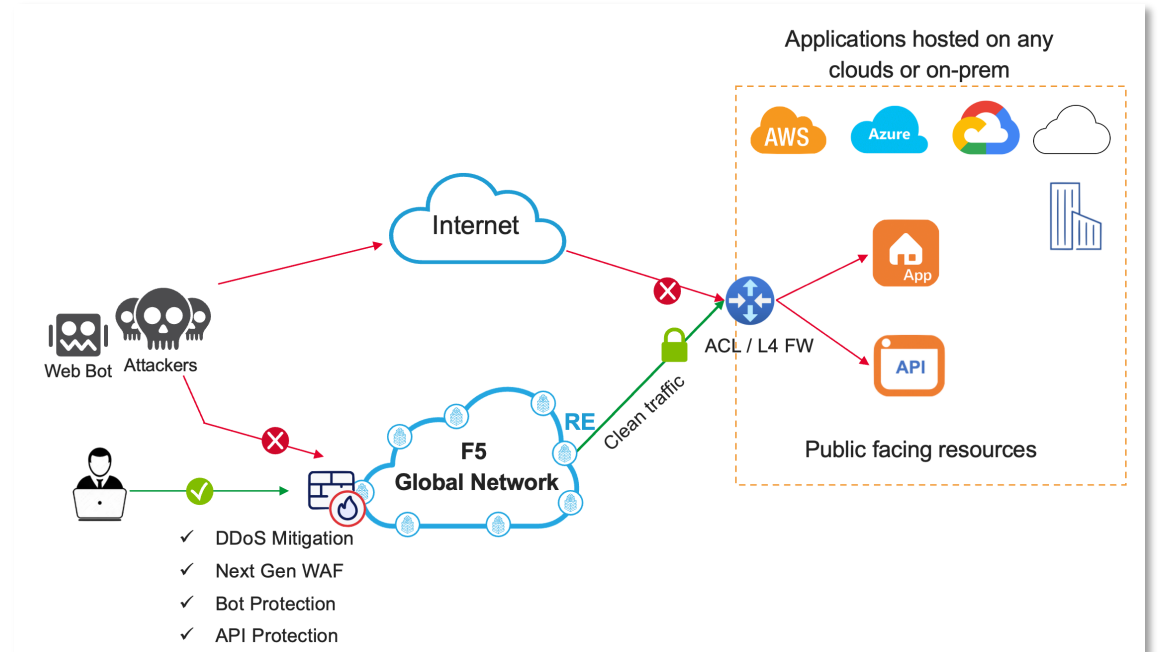
6. F5 XCのパブリックIP範囲をオリジンサーバ側のAllow Listsに追加し、他のIPアドレス範囲をブロックする

F5 XC WAAPをバイパスしたアクセスを防ぐため、オリジンサーバ側のセキュリティ機構（ルーター、ファイアウォール等）で、F5 XCのパブリックIP範囲からのみアクセスを許可するようにします。

F5 XCのパブリックIP範囲は、以下のページの“ Public IPv4 Subnet Ranges”を参照ください。

<https://docs.cloud.f5.com/docs/reference/network-cloud-ref>

この一覧は、新しい POP が構築されたときに更新されることがあります。



7. Malicious User Detectionを有効化（要オプション契約）

機械学習を活用したユーザの振る舞い検出により、不正ユーザからのアクセスを緩和することができます。

不正ユーザの識別には、送信元IP、TLS Fingerprint、Cookie、ヘッダや、その組み合わせを利用することができます。TLS Fingerprintと送信元IPをユーザ識別に使うと、誤検知を避けつつ、効果的な緩和処置を行えます。

お客様は、リスクベースアプローチに基づいて、以下のような緩和処置を構成できます。

- High Risk判定のユーザを、20分間ブロック
- Medium Risk判定のユーザには、CAPTCHAチャレンジ
- Low Risk判定ユーザにはJava Scriptチャレンジを

注: この機能の利用には、アドオンライセンスが必要です

The screenshot displays the Malicious User Detection configuration interface. It shows a timeline of activity for IP-216.173.99.29 and IP-89.42.201.131. The timeline includes risk scores and mitigation actions such as 'Blocking Temporarily' and '2 Request were from high risk IP 89.42.201.131 in last 33 seconds'. The configuration panel on the right shows settings for User Identification Policy, Malicious User Detection (Enabled), and Malicious User Mitigation And Challenges (Enabled). The Mitigation Settings are set to Custom, with a policy named 'arcadia-demo/mitigating-control'.

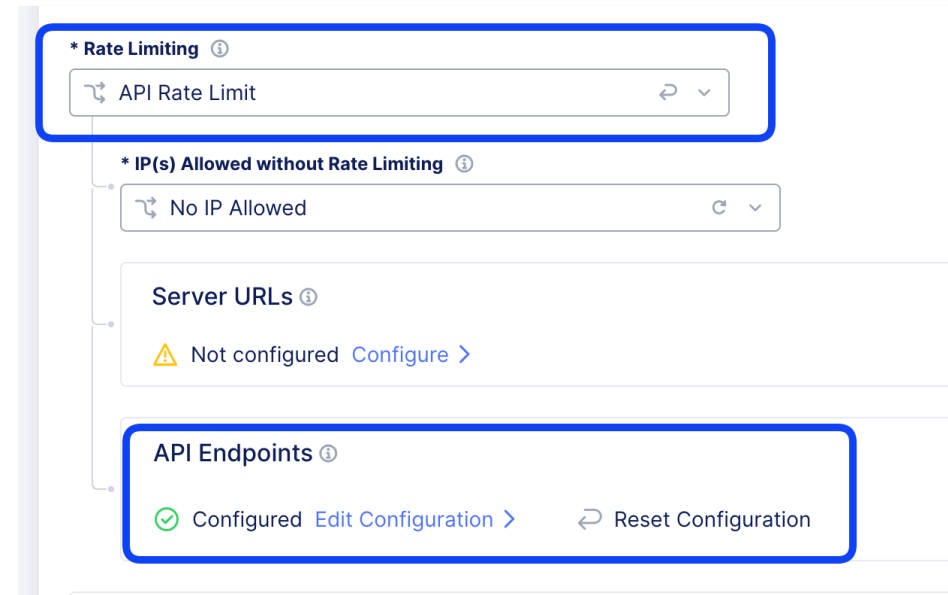
8. リソースを消費するワークロードに対して、Rate Limitingを有効化（要オプション契約）

オリジンサーバのリソースを著しく消費するようなアクセスポイントが存在する場合、それらに対して、レート制限を設定することを検討してください。

上記のようなアクセスポイントは、WAF機能等の緩和処置が動作する前に、リソースを飽和させる攻撃を受ける可能性があります。

また、本設定は、L7DDoS攻撃の防御にも有効です。

注: この機能の利用には、アドオン ライセンスが必要です

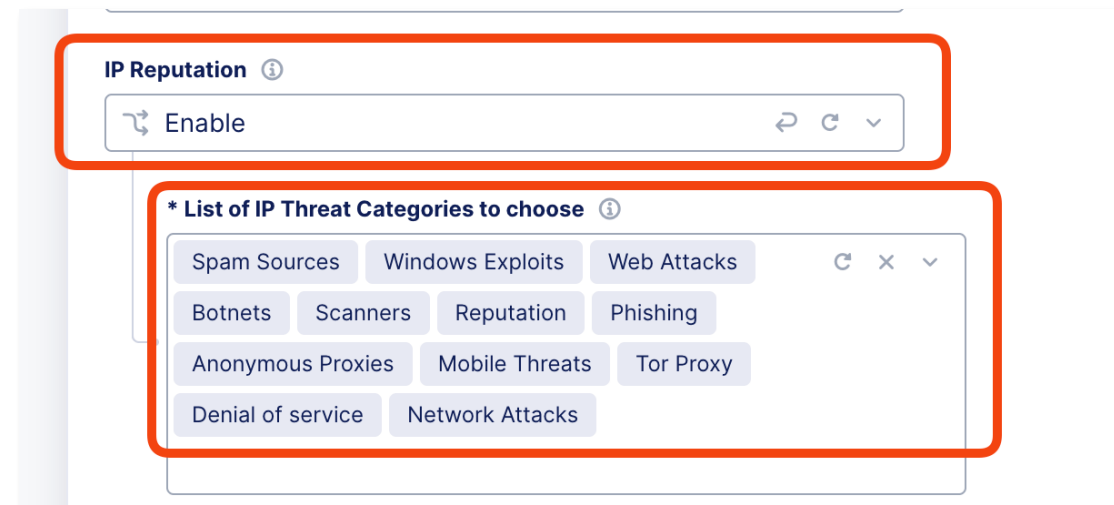


9. IP Reputation を有効化

レピュテーションスコアの低い既知のIPアドレス（Spam Source, ボットネット、Torプロキシなど）からのアクセスを遮断することができます。

レピュテーションデータベースは、随時更新されています。

レピュテーションスコアの低い既知のIPアドレスからアクセスを許可する特別な理由がない限り、設定を有効化することを推奨します。



10. L7DDoS Auto Mitigation機能の理解

高いエラー率や、応答遅延の発生などの異常なリクエストの動きを基に、L7DDoS攻撃が検知されると、この設定によって、送信元IPアドレスを元にした緩和処置が自動的に20分間、行われます。20分間の緩和処置期間が終わると、自動的に緩和処置は解除され、GUIのリスト表示からも削除されます。

L7DDoS Auto Mitigationは必ず有効化されており無効化できません。Default設定では、“Suspicious”判定した送信元はブロック、それ以外の送信元にはJavaScriptチャレンジが行われます。設定は、以下のように変更することができます。

The screenshot displays the AWS IAM console's DDoS Auto Mitigation interface. At the top, there are navigation tabs: Dashboard, API Endpoints, Malicious Users, Security Analytics, **DDoS**, Alerts, Requests, and Bot Defense. Below these, there are sub-tabs for Detections and **Auto Mitigations**. A search bar and a 'Refresh' button are visible. The main content area shows a table with 6 items. The table has columns for Name, IP Prefixes, Action, Created Time, and Expiry Time. Below the table is a world map showing the geographic distribution of the mitigated IP prefixes.

Name	IP Prefixes	Action	Created Time	Expiry Time
httpstat-ddos-lb-20231018022428-i3	5 Prefixes	Block	Oct 19, 2023, 6:41 AM	Oct 19, 2023, 7:01 AM
httpstat-ddos-lb-20231018021213-i3	203. [redacted] 9/32	Block	Oct 19, 2023, 6:40 AM	Oct 19, 2023, 7:00 AM
httpstat-ddos-lb-20231018022628-i3	203. [redacted] 9/32	Block	Oct 19, 2023, 6:40 AM	Oct 19, 2023, 7:00 AM

The screenshot shows the 'DoS Protection' settings for L7 DDoS Auto Mitigation. The settings are currently set to 'Default'. A dropdown menu is open, showing three options: 'Default', 'Block', and 'JavaScript Challenge'. The 'Default' option is selected.

DoS Protection

* L7 DDoS Auto Mitigation ⓘ

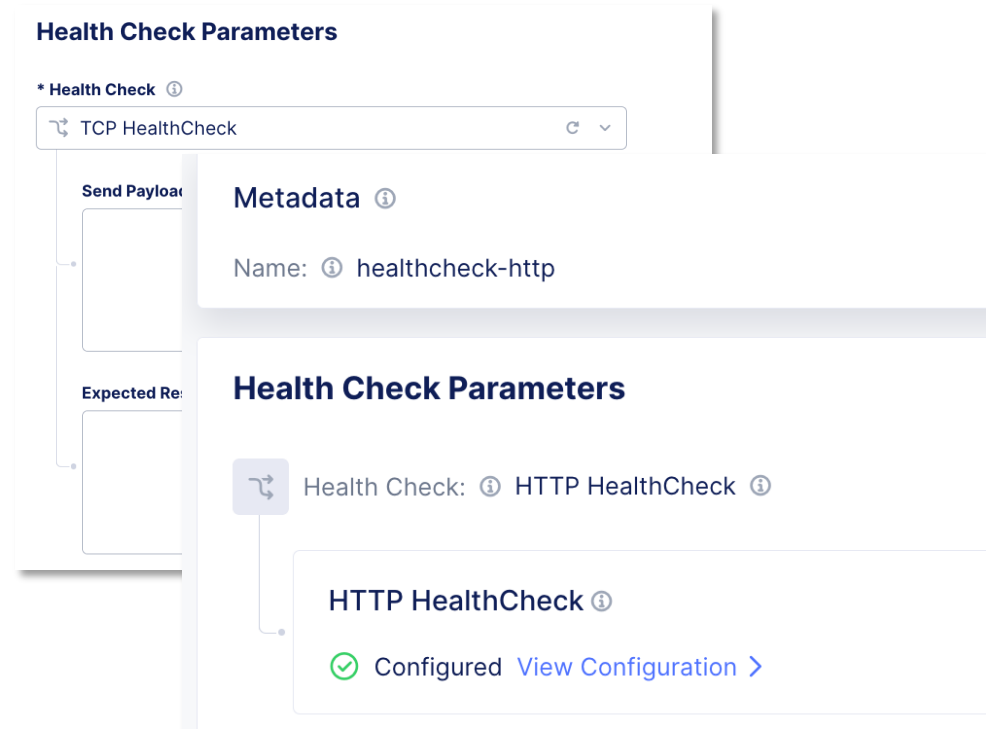
Default

- Default** (Default)
Block suspicious sources and serve JavaScript challenge to rest of traffic
- Block**
Block suspicious sources
- JavaScript Challenge**
Serve JavaScript challenge to suspicious sources

11. 適切なアプリケーションヘルスチェックの構成

HTTPヘルスチェックとTCPヘルスチェックを、正しく使い分けることを推奨します。

HTTPのアプリケーションに対して、TCPヘルスチェックを使用することはできますが、HTTPヘルスチェックを用いるほうが、実際のステータスをより適切に確認することができます。



12. Routes設定による柔軟な構成の実現

Routes機能によって、PATHやHTTP Methodを条件として、一致するリクエストを、指定のオリジンプールに転送したり、別のURLにリダイレクトしたり、HTTP LBから直接応答を返すといったことを実現できます。

The screenshot displays the configuration interface for a route. The settings are as follows:

- * Route Type**: Simple Route
- HTTP Method**: ANY
- * Path Match**: Prefix
 - * Prefix**: /
- Headers**: There are no items added yet. Start by adding first item. (Add Item button)
- Port Match**: No Port match
- * Origin Pools**:

Type	Name	Weight	Priority	Endpoint Subsets	Actions
Origin Pool	arcadia-frontend-pool	1	1		

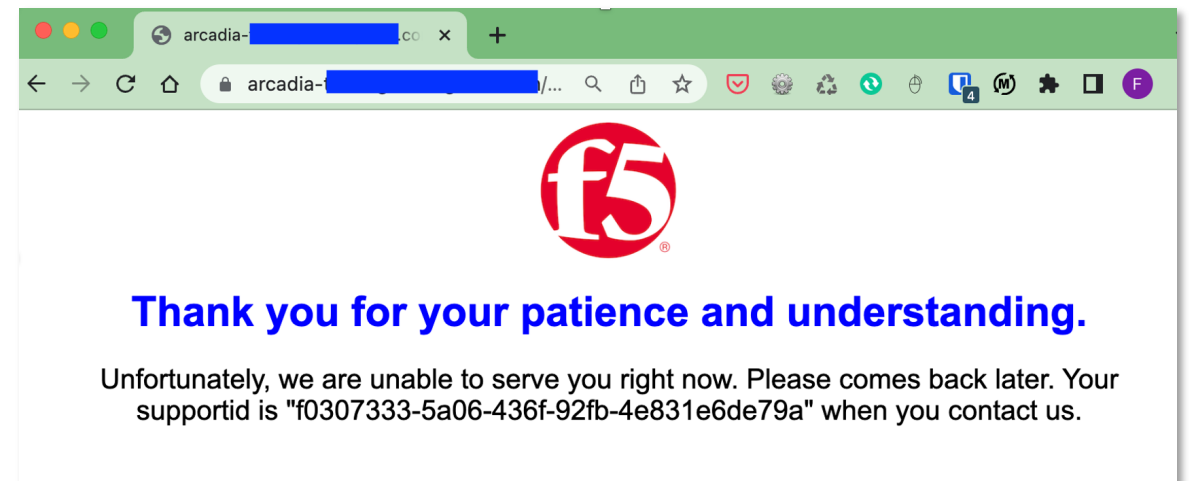
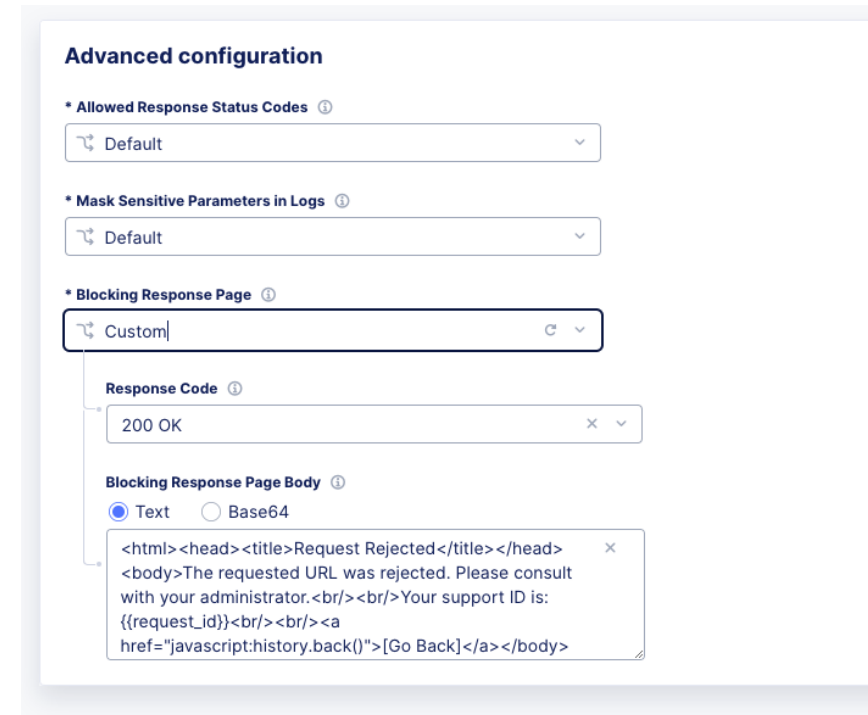
(Add Item button)
- * Host Rewrite Method**: Disable Host Rewrite
- Advanced Options**: Not configured [Configure >](#)

13. Blockingページのカスタマイズ

Blockingページには、必要最小限の情報を含めることが望ましいとされます。

F5 XC WAAPでは、Support IDと呼ばれるリクエストに一意的IDを表示されることがあります。このIDを表示しておくことで、リクエストがエラーになった際の問い合わせ対応をスムーズに行うことができます。

お客様は、このページをカスタマイズすることができます。デフォルトの応答コードは200(OK)であり、403(Forbidden)ではない点に注意してください。この応答コードについても、変更することは可能です。



14. アプリケーションのTimeout値とRetryポリシーのカスタマイズ

アプリケーションごとに、応答要件など通信に関する特定を持っています。

デフォルトでは、オリジンプール“Exception Handling”設定のConnection Timeoutは2秒（2,000msec）です。この設定により、宛先のオリジンサーバへの新規接続のタイムアウト値は2秒となります。F5XC HTTP-LB が2秒以内に、オリジンサーバから応答を得ない場合、F5 HTTP-LBは、クライアントに対して、503エラーを返します。オリジンサーバの負荷が高い際などに、503エラーの多発を回避したい場合に、本設定値を、例えば、10秒（10,000ms）などに変更する必要があるかもしれません。

デフォルトでは、F5 HTTP-LBのRetry回数は1回です。Routes設定のCustom Retry Policyにて、必要に応じて変更することができます。

Exception Handling

Connection Timeout (ms) ⓘ

10000

HTTP Idle Timeout (ms) ⓘ

300000

Miscellaneous Options

* Select Retry Policy ⓘ

Custom Retry Policy

* Custom Retry Policy ⓘ

✔ Configured with default values [View Configuration >](#)

Number of Retries ⓘ

1

15. App Firewall(WAF)のBlocking Modeでの運用

セキュリティの観点からは、AppFirewall(WAF)をBlockingモードで運用することが望ましいです。誤検知(False Positive)は、XCコンソール上から、簡単に除外設定できます。

AppFirewallのデフォルトのポリシーでは、“High”と“Medium”の精度のシグネチャが選択されています。これは、効果と誤検知のバランスを考慮した選択です。

お客様は、“High”と“Medium”、“Low”の3つの精度のシグネチャを組み合わせることでポリシーを作成することができます。

また、検出対象の“Attack Type”は全て有効となっています。お客様は、必要に応じて、個別の“Attack Type”を無効にすることができます。

The screenshot shows the configuration page for an App Firewall rule. The 'Enforcement Mode' dropdown menu is highlighted with a pink box and is currently set to 'Blocking'. Other visible fields include 'Name' (corp-waap-high-to-medium), 'Labels' (Add Label), and 'Description'.

block	arcadia.apac-sp.f5demos.com	/	⋮
allow	arcadia.apac-sp.f5demos.com		<ul style="list-style-type: none">+ Create WAF Exclusion rule+ Add to Blocked Clients+ Add to Trusted Clients
block	arcadia.apac-		

16. レポート機能の活用

レポート機能により、サービスの概要スナップショットを配信できます。
要件に応じた定期的な配信頻度で、受信者に電子メールでの送信が可能です。



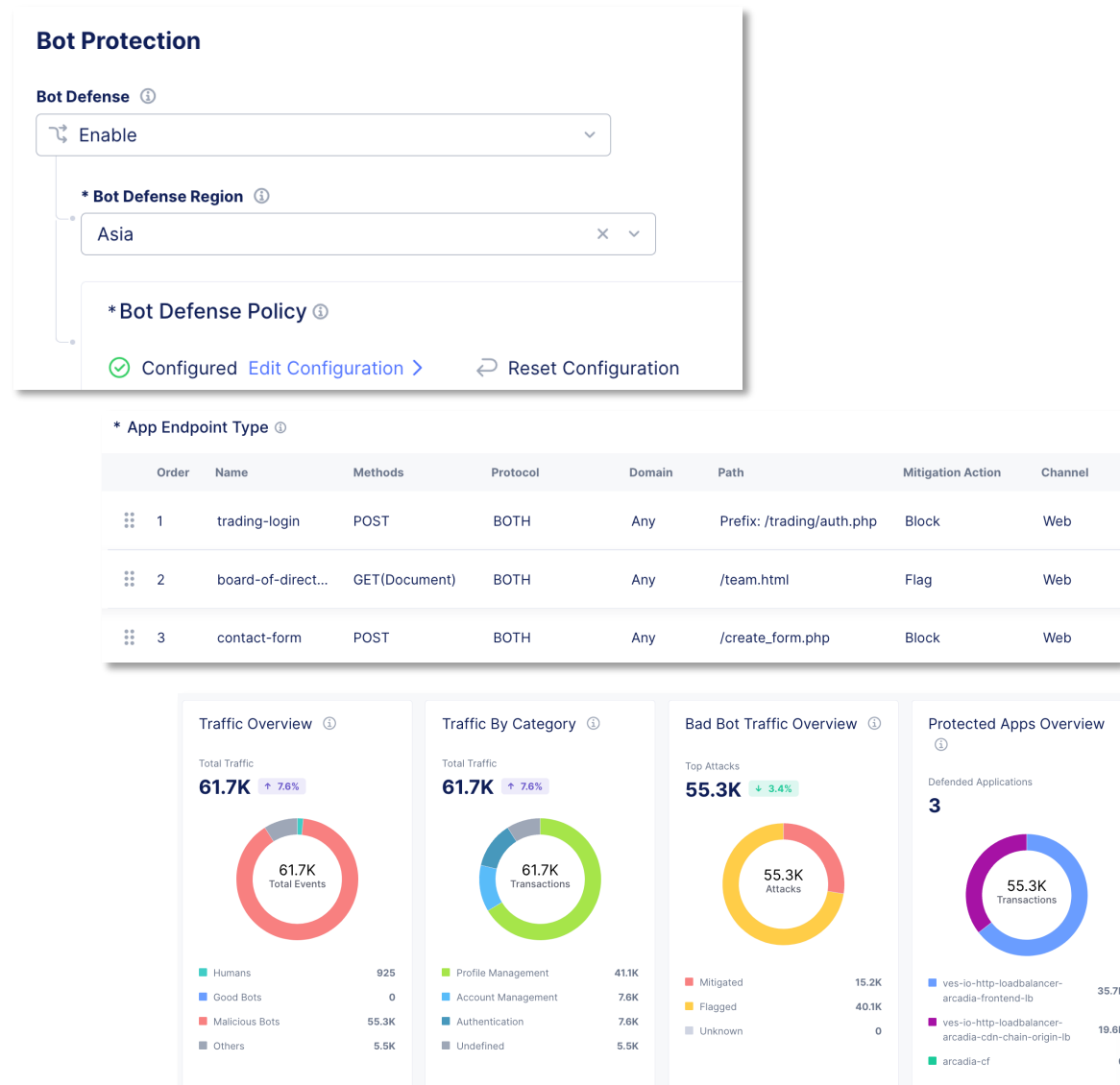
17. Bot Defenseの活用（要オプション契約）

Bot Defenseは、クライアント側から詳細なテレメトリ情報を収集し、それをもとに、リクエストが自動化されたものか否かを高精度に判定します。本機能により、アカウント乗っ取り等の高度な不正行為を行う高機能なボットを検出、緩和できます。

テレメトリの収集は、ブラウザの場合はJavaScript、ネイティブモバイルアプリの場合は、SDKにて行います。

自動化と判定されたリクエストは、リダイレクトもしくはブロック処置をF5 XC HTTP LBにて行い、オリジンサーバに到達する前に緩和処置を行います。

注: この機能の利用には、アドオンライセンスが必要です



18. Synthetic Monitoringの活用によるMTTR(平均修理時間)の削減

F5 XC Synthetic Monitoringは、HTTP(S)リクエストとDNSクエリを生成し、アプリケーションの健全性をチェックする外形監視サービスです。

アップタイム、性能、ヘルスチェック分析などにより、アプリケーションの健全性の定量化/可視化や、アラートの通知機能により、MTTR(平均修理時間)を短縮します。

監視元として、F5XCのPoPとAWSのRegionを指定でき、複眼的データの採取が可能です。

注:

本機能は、500,000(500K)回/月間までBase Packageのライセンス内で利用可能です。

例えば、一つのHTTP(S)アプリケーションの監視を1つの監視元から、1分間隔で行う場合は、約43,200回の実行となります。

