Next WAF セットアップガイド

F5 ネットワークスジャパン合同会社

2024 年 05 月 13 日

目次:

第 1 章　はじめに 3

第 2 章　コンテンツ 5

2.1 BIG-IP Next WAF ハンズオン概要 6

2.2 WAF ポリシーの作成とデプロイ 7

2.3 シグネチャのアップデート 23

最終更新日: 2024 年 x 月 xx 日

第 1 章

はじめに

このページでは、これらのオフィシャルなドキュメントの補足となる資料や、複数の機能を組合せてソリューションを実現する方法をご紹介いたします。F5 のオフィシャルなドキュメントはこちらにございます。

- MyF5: https://my.f5.com/manage/s/
- F5 Cloud Docs: https://clouddocs.f5.com/
- F5 DevCentral（コミュニティ）: https://community.f5.com/

第 2 章

コンテンツ

こちらのページでは、以下の内容をご紹介しております。

- 本セットアップガイドにて、F5 BIG-IP Next WAF（以下"Next WAF"）のポリシーの設定方法についてご案内します。
- Next WAF は、Web アプリケーションファイアウォールです。
- Next WAF によって、Web アプリケーション特有の攻撃に対する防御が可能となります。
- Bot 対策機能、L7 レベルの DoS 攻撃に対する防御機能も兼ね備えています。
- 本ガイドでは、Next WAF をご購入いただいてすぐに WAF を導入頂けるように、必要となる典型的なセットアップ手法を、豊富なスクリーンショットを交えて解説します。（実際は環境構成にあった設定値を設定して下さい。）
- 本ガイドでは、F5 Japan におけるハンズオントレーニングのコースでも利用しております。

注釈: 本ドキュメントの手順は、F5 UDF (Universal Demonstration Framework) というラボ環境での実施を前提に書かれています。UDF 以外での環境で利用される場合は、IP アドレス等は環境に合わせて読み替えてください。

注釈: 設定手順において、スクリーンショットを撮った環境や時期により、スクリーンショット内の値とガイド内で指示される値が異なる箇所があるかもしれませんが、ご容赦ください。

2.1 BIG-IP Next WAF ハンズオン概要

本章では、BIG-IP Next WAF とハンズオン環境の概要についてご紹介致します。

BIG IP Next の概要を学習したい場合は、以下を参照ください。

https://f5j-easy-setup-next-ltm.readthedocs.io/ja/latest/content01/module02/module02.html

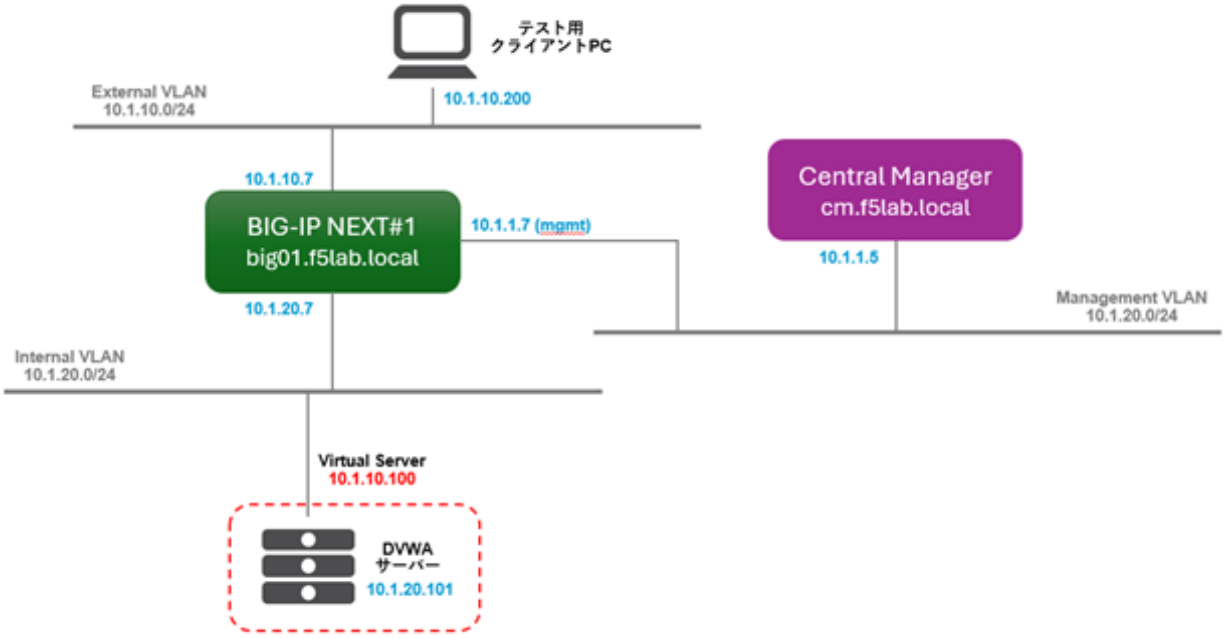
2.1.1 BIG-IP Next WAF とは

F5 BIG-IP Next WAF とは、OWASP TOP10 の攻撃、ウェブアプリケーションの脆弱性、ゼロデイ攻撃、L7 レイヤの DDoS 攻撃などから WEB アプリケーションを守る高度なウェブアプリケーションファイアウォールです。

BIG-IP Next WAF は、堅牢なセキュリティ ポリシーを作成することによって、有効なアプリケーション トランザクションのみを許可し、バッファ オーバーフロー、SQL インジェクション、クロスサイト スクリプティング、パラメータ改ざん、Cookie ポイズニング、Web スクレイピングなどの対象となるアプリケーション層の脅威から Web アプリケーションを保護します。ポジティブセキュリティ モデルを使用して、検証されたユーザー セッションとユーザー入力、および有効なアプリケーションの応答の組み合わせに基づいてアプリケーションを保護します。また、セキュリティ ポリシーテンプレートにより、一般的なアプリケーションをシンプルかつ迅速に保護できる仕組みを提供しています。

2.1.2 ハンズオン環境ネットワーク構成

BIG-IP Next WAF ハンズオンのシナリオでは以下のネットワーク環境を構築します。

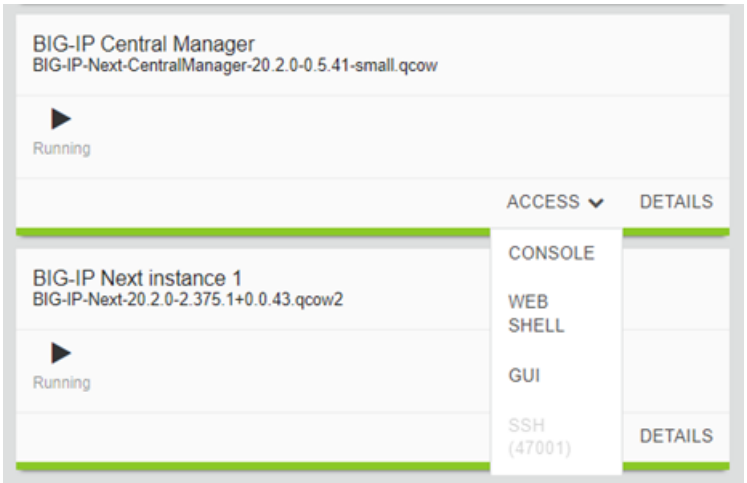


2.2 WAF ポリシーの作成とデプロイ

本章では、BIG-IP NEXT の Central Manager (CM) から WAF ポリシーを作成し、脆弱なアプリケーションにアサインすることによって脅威から保護します。

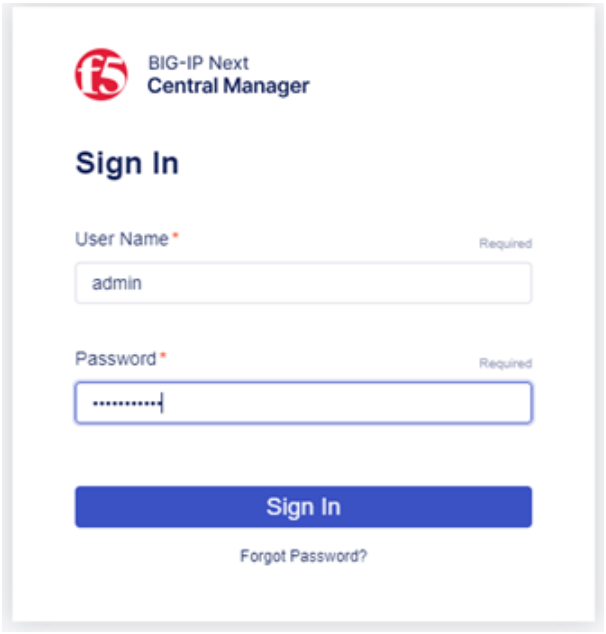
2.2.1 脆弱なウェブサーバーをデプロイ

UDF 画面上部タブの"DEPLOYMENT"をクリックし、BIG-IP Next Central Manager インスタンスの"ACCESS" > "GUI" を選択します。

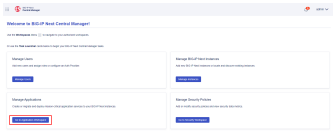


BIG-IP Next CM GUI へのログイン、ログインプロンプトが表示されたら、ユーザ名/パスワードを入力してログインします。

- ユーザー名/パスワード:
- **admin/Welcome123!**



ログインすると次のようなホーム画面から"Manage Applications"をクリックします。



“ Add Application ”をクリックして、新規アプリケーション作成します。

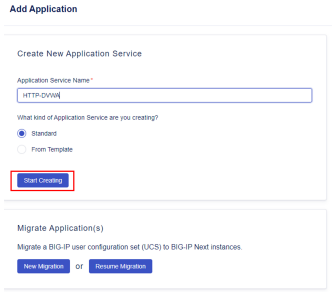
Application Service Name:

- **HTTP-DVWA**　（任意の名前）

What kind of Application:

- **Standard**　を選択

- **“ Start Creating ”**を二回クリック



“ Pools ”を選択し、“ Create ”をクリックして pool の名前とポート番号を入力します。

Pool Name:

- **dvwa_pool**

Server Port:

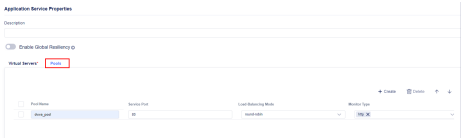
- **80**

Load-Balancing Mode:

- **round-robin**

Monitor Type:

- **http**



"Virtual Servers"の tab に戻り、以下内容を入力します。

Virtual Server Name:

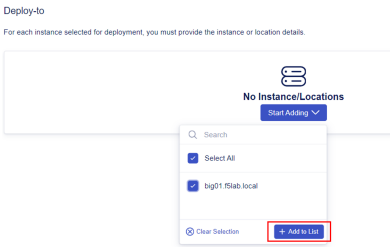
- **DVWA-VS**

Pool:

- **dvwa_pool**　(先ほど作成されました pool を選択)

- **“ Review & Deploy ”** をクリック

次の画面から"Start Adding"をクリック、“ big01.f5lab.local ” のチェックボックスをチェックしてから"Add to List"をクリックします。

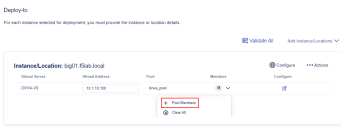


次の Deploy 画面で、Virtual Server の IP と Pool member を設定します。

Virtual Address:

- **10.1.10.100**

- Members の下矢印を展開し、 “ +Pool Members ” をクリック



“ +Add Row ” を 2 回クリック pool member を作成します。

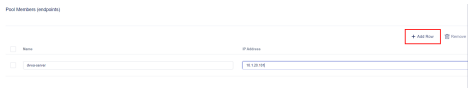
Name:

- **dvwa_server**

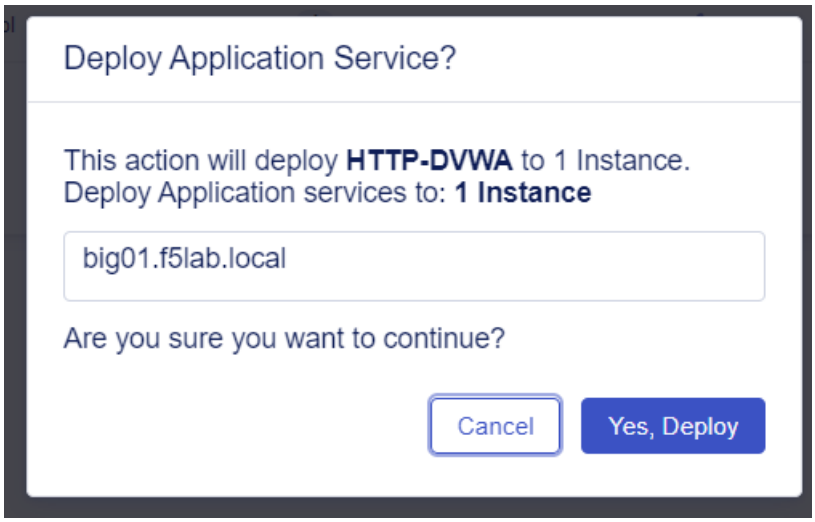
IP Address:

- **10.1.20.101**

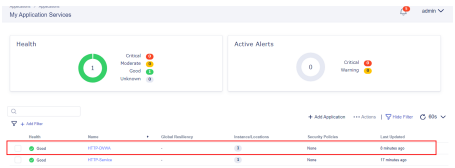
- 入力後、 ” Save ” をクリック



設定内容に問題ないかを適用前に"Validate All"で検証し、エラーがなければ"Deploy Changes"をクリックして本番適用します。

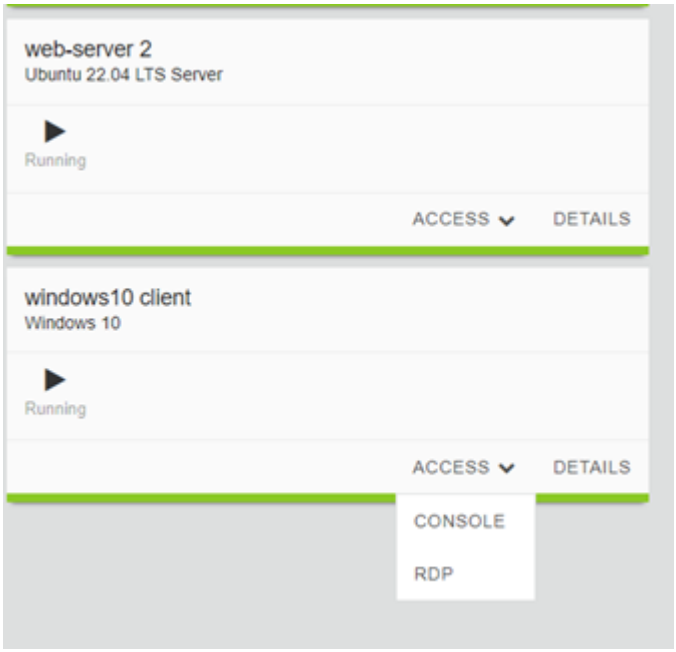


デプロイ完了後、Dashboard から作成されたアプリケーション"HTTP-DVWA"を確認出来ます。



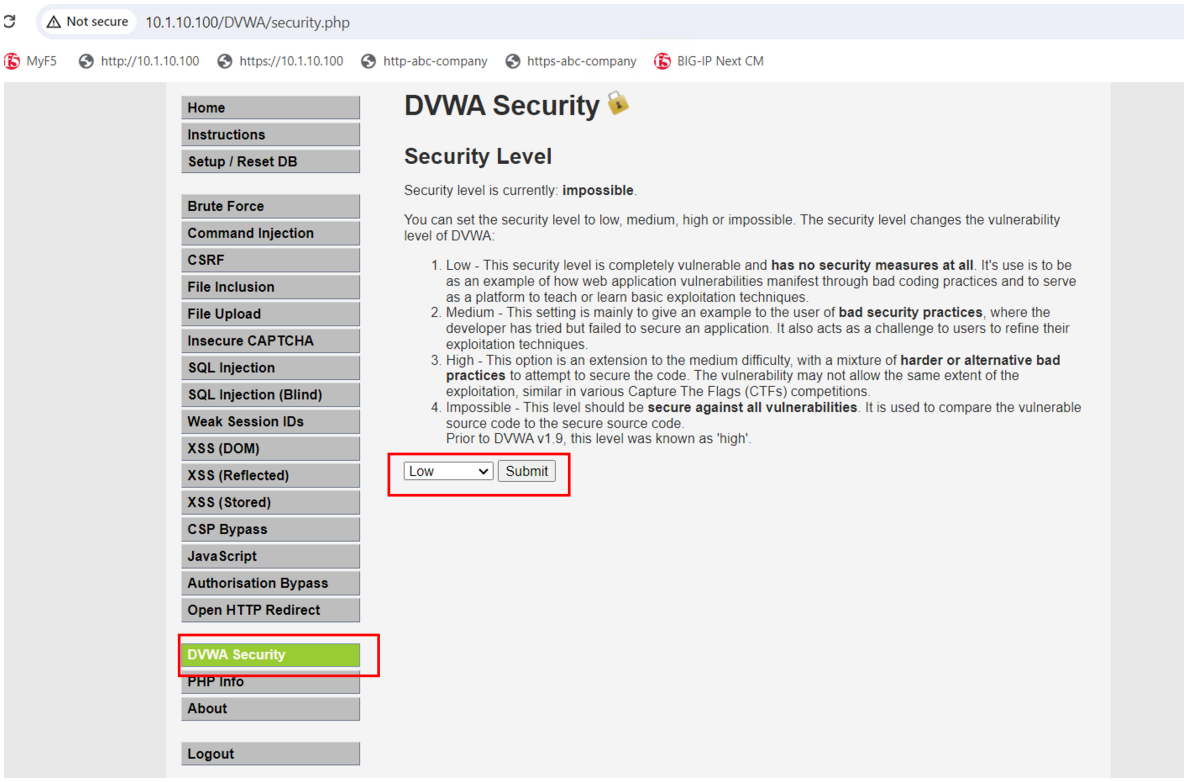
UDF **環境から** Windows **クライアントを起動します。**

- ユーザー名/パスワード:
- **user/user**

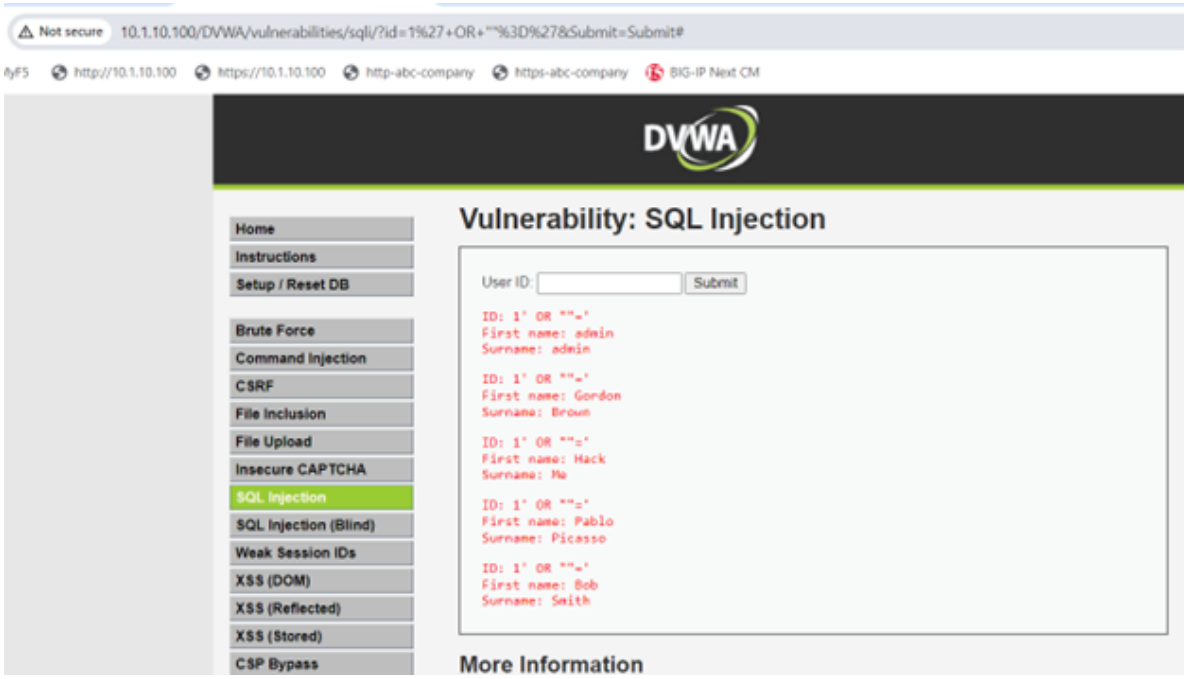


Chrome ブラウザを開き、http://10.1.10.100/DVWA/login.php にアクセスします。Username: admin、Password: password でログインします。

DVWA Security にアクセスし、Security Level を Low に設定します。

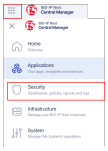


SQL Injection にアクセスし、User ID に 'or 1=1 # と入力し、SQL インジェクション攻撃をします。(本ガイドからコマンドはコピーしないで下さい。シングルクォーテーションに注意してタイプして下さい。)

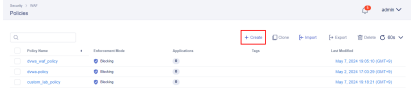


2.2.2 WAF ポリシーを作成してアプリケーションへ適用

CM 画面左上部の workspace から、” Security ” を選択します。



画面左側で"WAF" > "Policies"を選択、"Create"をクリックしてポリシーを新規作成します。



Name:

- **dvwa_waf_policy**　（任意の名前）

• Advanced View を enable します　（テンプレート選択のため）

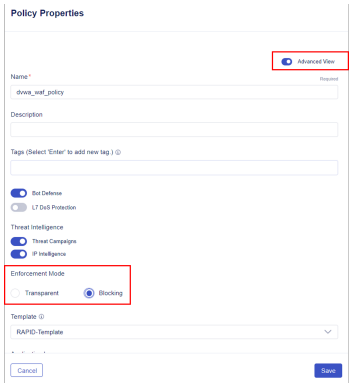
Template:

- **RAPID-Template**

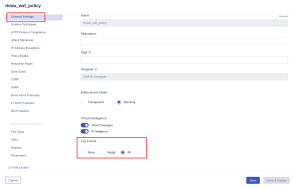
Enforcement Mode:

- **Blocking**

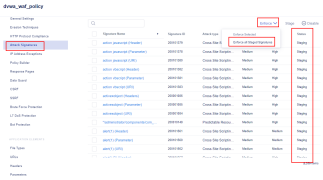
• “ Save ” をクリックします

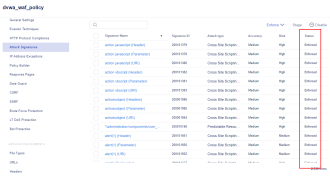


作成された WAF ポリシーを選択、” General Settings ” から ” Log Events ” を ” All ” にし、” Save ” をクリックします。



"Attack Signatures"のページを選択し、"Enforce" > "Enforce all Staged Signatures"でシグネチャの staging を解除します。





CM 画面左上部の workspace から、"Applications"へ戻ります。先ほど作成したアプリケーション (HTTP-DVWA) を選択し、"Edit"します。

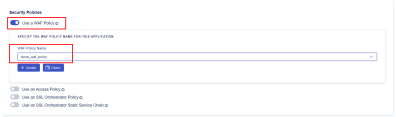
“ Security Policies ”の編集マークをクリックします。

- “ Use a WAF Policy ” を enable します

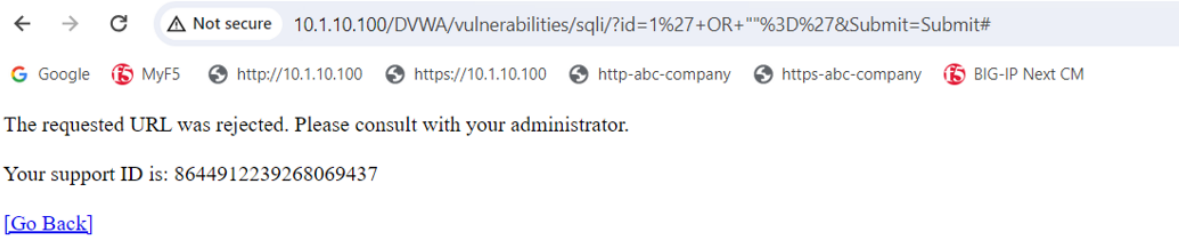
WAF Policy Name:

  - **dvwa_waf_policy** (先ほど作成した WAF ポリシー)

- “ Save ” をクリックします
- “ Review & Deploy ” > “ Validate All ” > “ Deploy Changes ” で WAF ポリシーをアプリケーションへ適用します



Windows クライアントから DVWA の SQL Injection ページより、User ID に 'or 1=1 # と入力し、SQL インジェクション攻撃をします。攻撃が reject されたことを確認します。

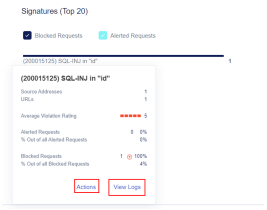


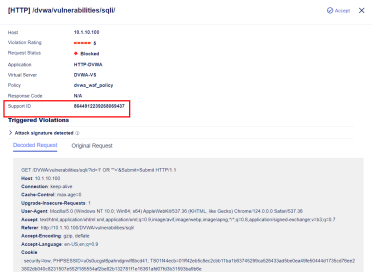
2.2.3 セキュリティイベントの確認とシグネチャのチューニング

誤検知などが発生した場合の対処例をご紹介します。以下で実施する内容は、Web アプリケーションの各パラメータの役割が全て把握できている場合を除き、運用開始前から全てを設定するのは難しいかもしれません。その場合は、仮運用・本運用に入ってから、チューニングが簡単に実施可能です。

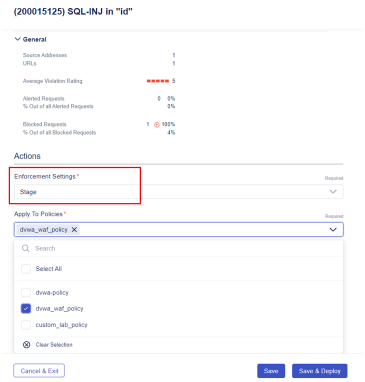
CM 画面左上部の workspace から、” Security ” を選択します。“ WAF Dashboards ” からセキュリティモニタリング情報を確認します。“ Polices ” からポリシーごとにセキュリティイベントに対してフィルターかけます。

“ Signatures ” から先ほど reject された sql injection リクエストをクリックし、” View Log ” から詳細 log を確認可能です。(クライアント PC のブラウザ上のリスポンスから表記された SupportID を log 中の SupportID を比較することでイベントログを特定出来ます。)

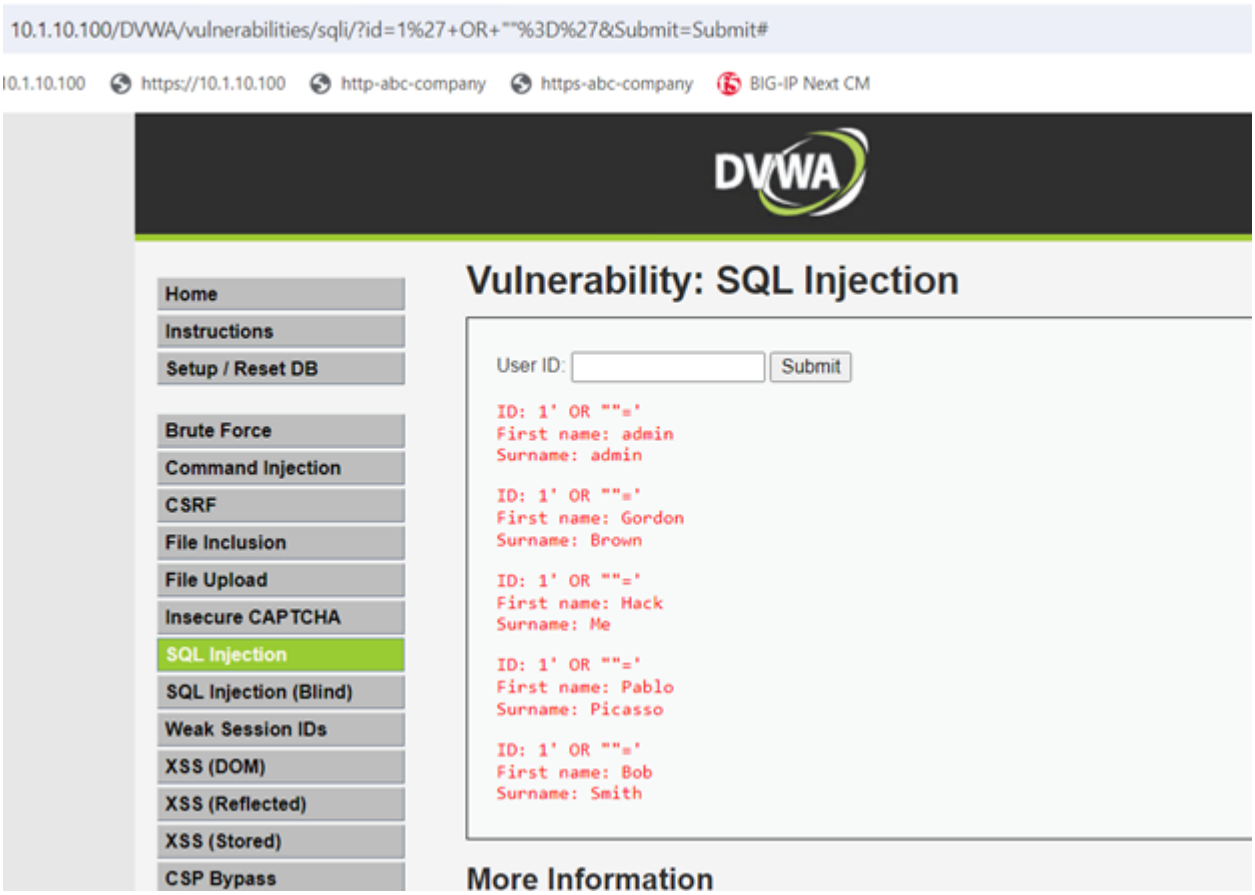




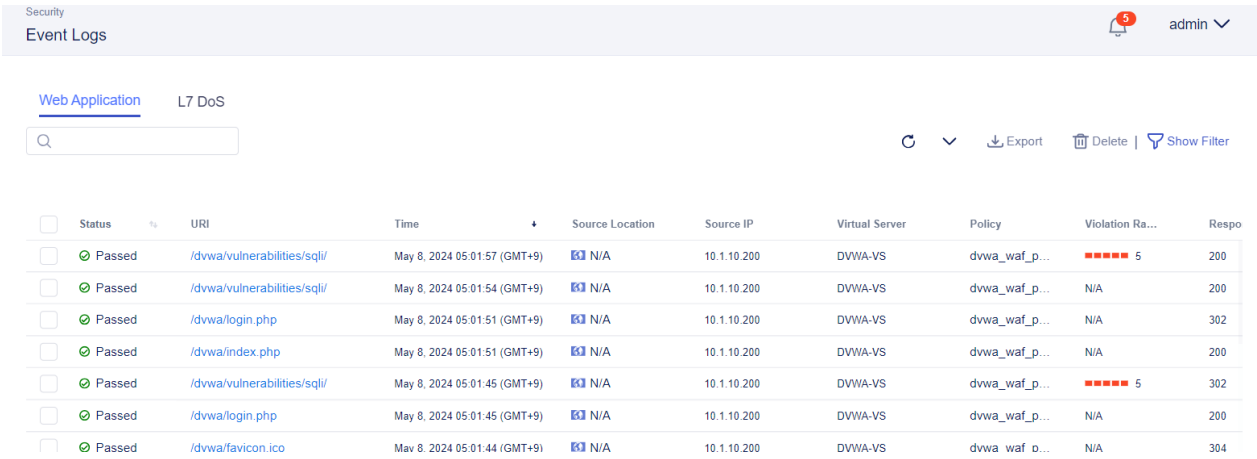
“ Actions ”をクリックすると、シグネチャごとで enforcement setting を特定ポリシーに対して override することが出来ます。



“ Save ” > “ Deploy ”でシグネチャの override を適用して、クライアントから再度 SQL インジェクション攻撃をする際、リクエストは reject されません。



また、Event Logs からはリクエストログを確認出来ます。

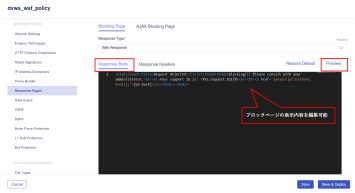


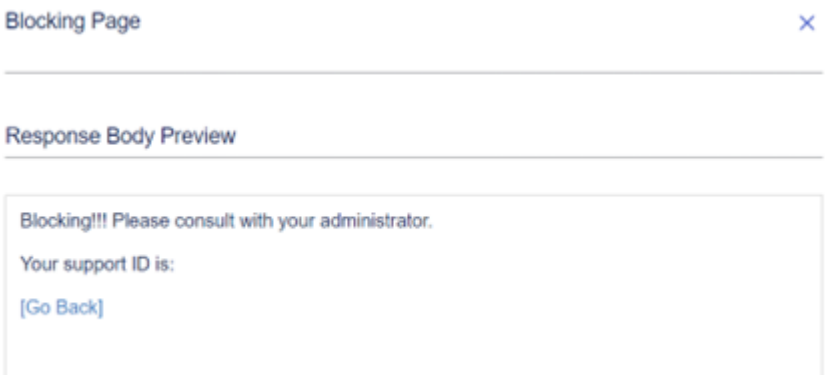
2.2.4 Blocking 画面のカスタマイズ

攻撃をブロックした際、ユーザに返されるレスポンスページの内容をカスタマイズすることが可能です。

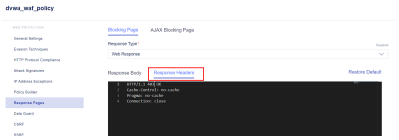
CM 画面左上部の workspace から、"Security"を選択します。WAF > WAF Policys より、適用したい WAF ポリシーを選択して、"Response Pages"の設定ページを選択します。

Response Body でブロックページの内容をカスタマイズすることが出来ます。"Preview"をクリックすることで、ブロックページのレビューが表示されます。クライアントから攻撃を行う際、カスタマイズされた内容がブラウザで表示されます。





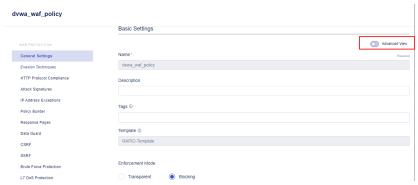
また、必要に応じて、Response Headers をカスタマイズする（eg. response code を 200 から 403 へ変更など）や、ブロックページを指定 URL へ Redirect することも設定可能です。



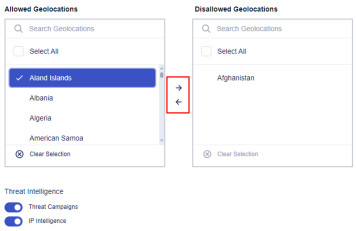
2.2.5 Geolocation の設定

WAF ポリシーに保護されているアプリケーションに対して、Geolocation Enforcement を使用して特定の国でのアプリケーションの使用を制限または許可できます。デフォルトでは、すべての地理位置からのアクセスが許可されます。Geolocation の設定を行うことで、接続される予定のない国からの接続をブロックすることが可能です。

CM 画面左上部の workspace から、"Security"を選択します。 WAF > WAF Policys より、適用したい WAF ポリシーを選択して、"General Settings"の設定ページを選択します。“ Advanced View ” を Enable します。



設定画面の Allowed Geolocations / Disallowed Geolocations の指定により、ブロックしたい地理位置を設定して“ Save & Deploy ”します。



その他、ポリシーの詳細カスタマイズ方法は以下の記事をご確認下さい。

- Customize a WAF Policy

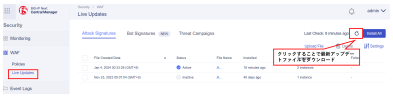
2.3 シグネチャのアップデート

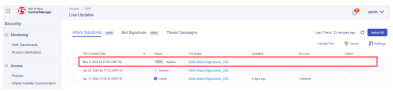
F5 は、Attack Signature, Bot Signature と Threat Campaigns 更新を頻繁にリリースします。 これらの更新には、新しいエントリと既存のエントリの機能強化が含まれます。

本章は、Attack Signature など Live Upates を適用する方法を紹介します。

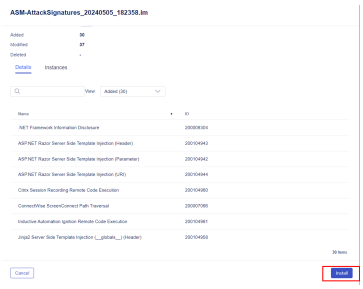
2.3.1 Live Updates の設定と適用

CM 画面左上部の workspace から、"Security"を選択します。WAF > Live Updates > Attack Signatures を選択し、リフレッシュマークをクリックすることで、最新のアップデートをダウンロードします。



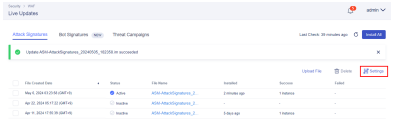


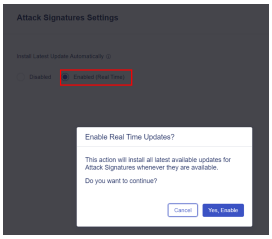
最新のファイルネームを選択し、” Install ” をクリックしてアップデートを適用します。



インストール完了後、最新のファイルの Status が Active になります。

また、Settings で Install Latest Update Automatically の設定を Enabled (Real Time) へ変更すると、手動で最新のアップデートファイルを取得することが不要で、アップデートファイルが定期的にダウンロードされます。





以上 Automatically アップデートは Attack Signatures, Bot Defense, Threat Campaigns ごとで設定されます。必要に応じて該当 tab を選択する上、設定してください。