
AWAF v17.1 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 01 月 23 日

目次:

第 1 章	はじめに	3
第 2 章	コンテンツ	5
2.1	AWAF 設定初級編	5
2.2	AWAF 設定中級編	73

最終更新日: 2023 年 8 月 28 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ます。

- 本セットアップガイドにて、F5 Advanced WAF (以下、AWAF) のポリシーの設定方法についてご案内します。
- AWAF は、Web アプリケーションファイアウォールです。
- AWAF 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、AWAF 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。

2.1 AWAF 設定初級編

本章では、基本的な AWAF の設定内容についてご紹介致します。

2.1.1 AWAF とは

F5 Advanced WAF (略して AWAF) 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。

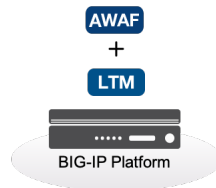
AWAF であれば、スタンドアローン構成、BIG-IP LTM (ADC) にアドオンして利用する構成を取ることが可能です。そして、オンプレでも、Public Cloud でも Private Cloud でも動作するため、デプロイ場所を選びません。

自社で柔軟な WAF ポリシーを作成したいお客様、AWAF を利用して高度な WAF サービスを提供したいというサービス事業者様、そして、LTM 導入済みで WAF を追加したいお客様など、幅広くご利用頂けます。

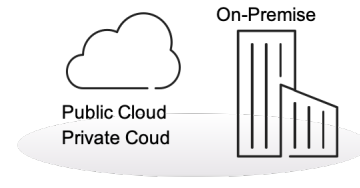
スタンドアロン構成



LTMにアドオン構成



デプロイ場所を選ばない



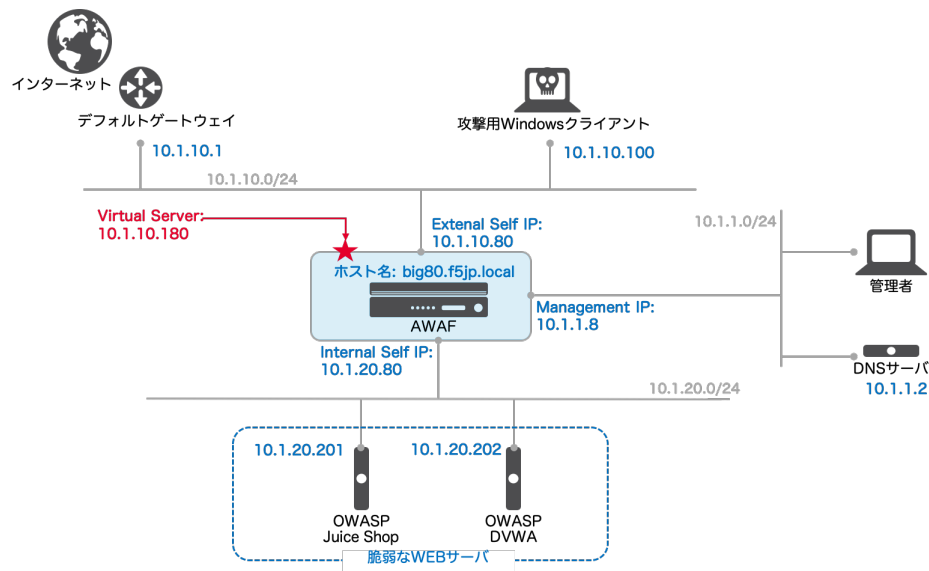
その他、AWAF の特長や利用メリットは以下の記事をご確認下さい。

- [K85426947: BIG-IP ASM operations guide](#)
- [K07359270: Succeeding with application security](#)

2.1.2 AWAF スタンドアロン構成ネットワークサンプル

本手順書では以下のサンプルネットワーク構成で設定を行います。(F5 ハンズオン環境でも同様のネットワーク構成を利用しています。)

1. 本ガイドにおける構成イメージ

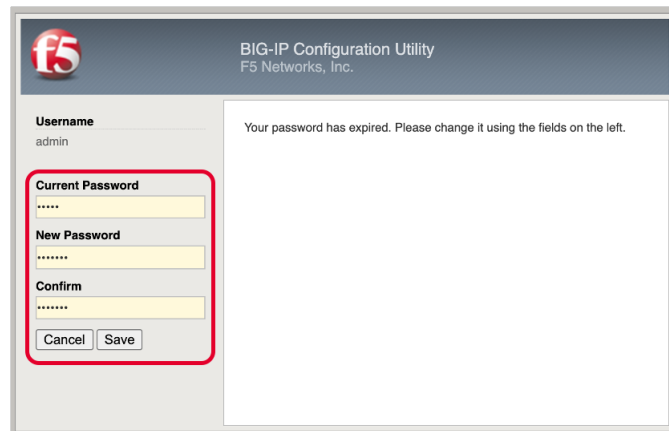


注釈:

- v17.1.0.2 以上のバージョンをご利用下さい。
- (各 F5 代理店でサポート可能な範囲において、) 極力最新のバージョンを適用頂くことをおすすめ致します。最新のバージョンは AskF5 でご確認ください。

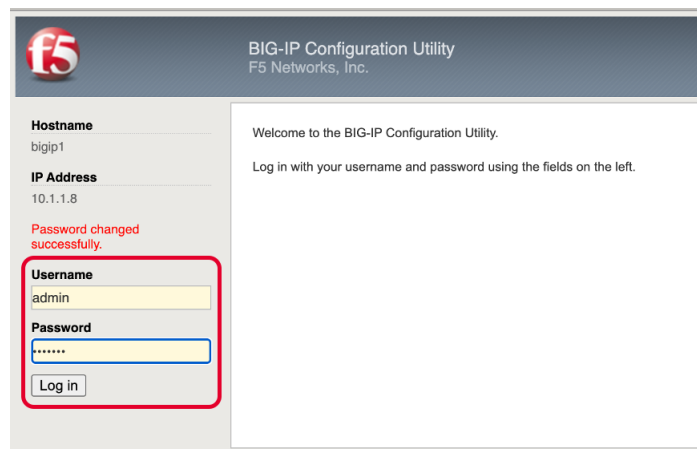
2.1.3 初期設定（プロビジョニング、ネットワークの設定等）

1. 初期パスワード（Username:admin, Password:admin）でログインし、F5 ハンズオントレーニングではパスワードを（ilovef5）に変更します。



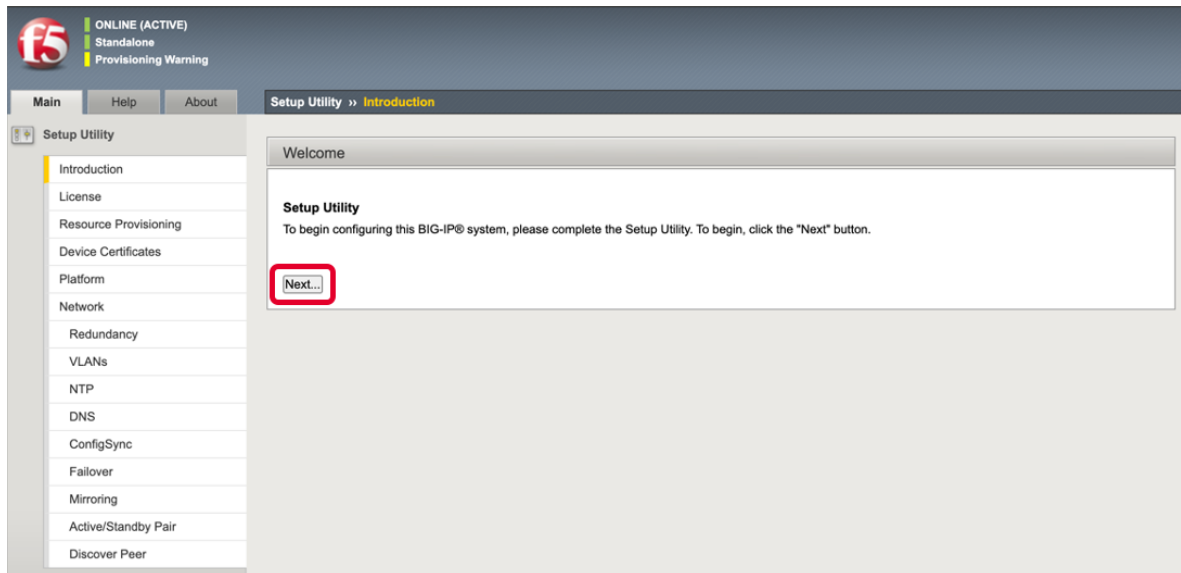
The screenshot shows the 'BIG-IP Configuration Utility' interface by F5 Networks, Inc. On the left, the 'Username' is set to 'admin'. Below it, a red box highlights the password change fields: 'Current Password', 'New Password', and 'Confirm', each with a masked input field. At the bottom of this box are 'Cancel' and 'Save' buttons. On the right, a message states: 'Your password has expired. Please change it using the fields on the left.'

2. パスワード変更に成功したら、変更後のパスワード（Username:admin, Password:ilovef5）でログインします。

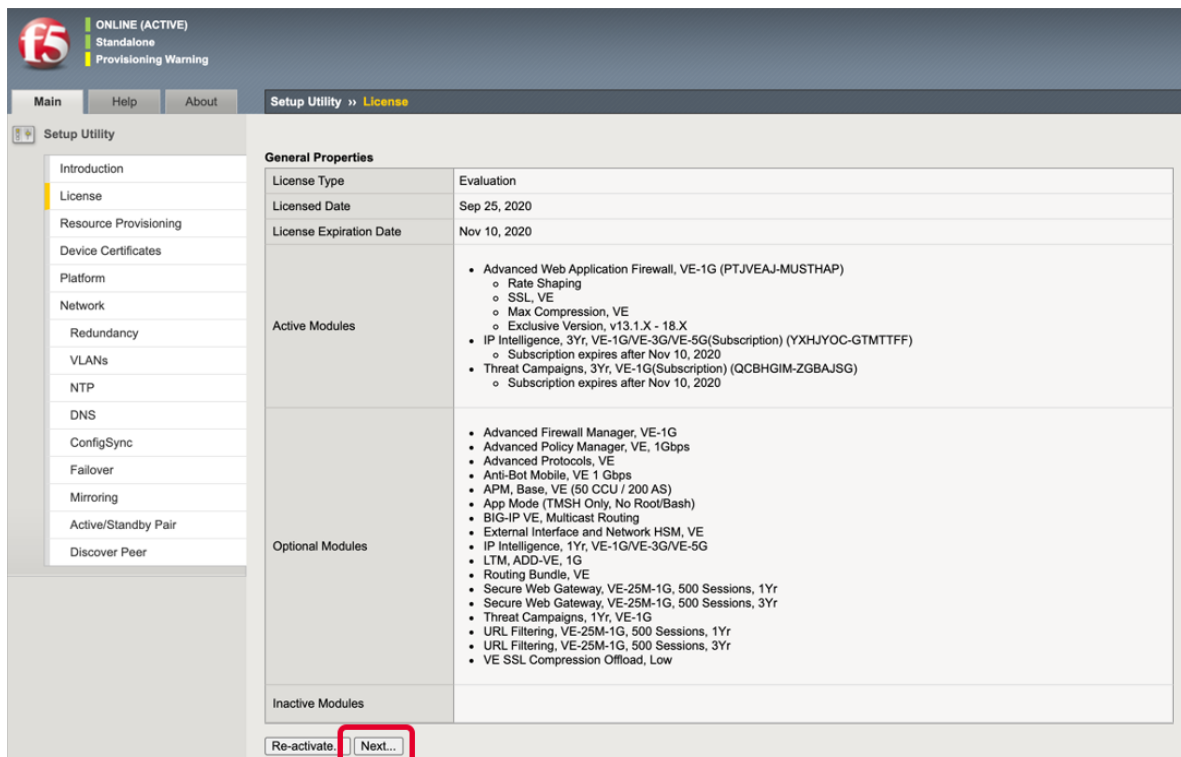


The screenshot shows the 'BIG-IP Configuration Utility' interface. On the left, the 'Hostname' is 'bigip1' and the 'IP Address' is '10.1.1.8'. A red message indicates 'Password changed successfully.'. Below this, a red box highlights the login fields: 'Username' (set to 'admin') and 'Password' (masked). A 'Log in' button is at the bottom of the box. On the right, a welcome message says: 'Welcome to the BIG-IP Configuration Utility. Log in with your username and password using the fields on the left.'

3. *Next* ボタンを選択します。



4. ライセンスアクティベーションを行います。ライセンス投入済みの場合は、*Next* ボタンを選択します。

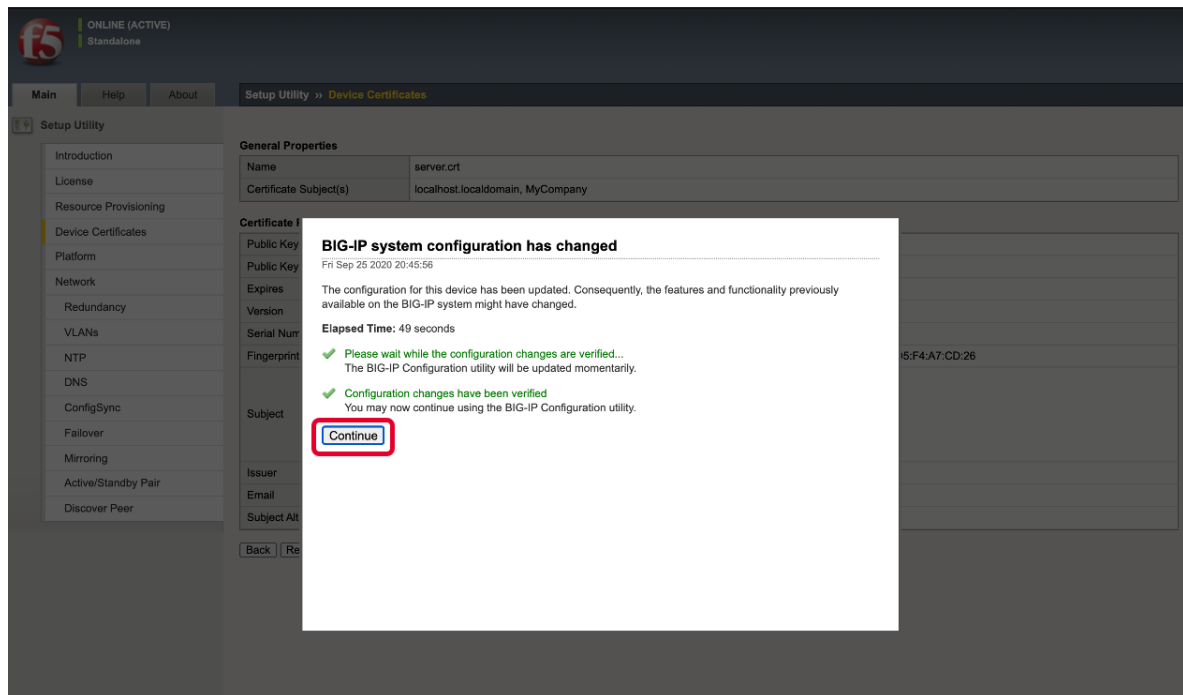


5. プロビジョニングを行います。Application Security(ASM) のみを選択し、*Next* ボタンを選択します。

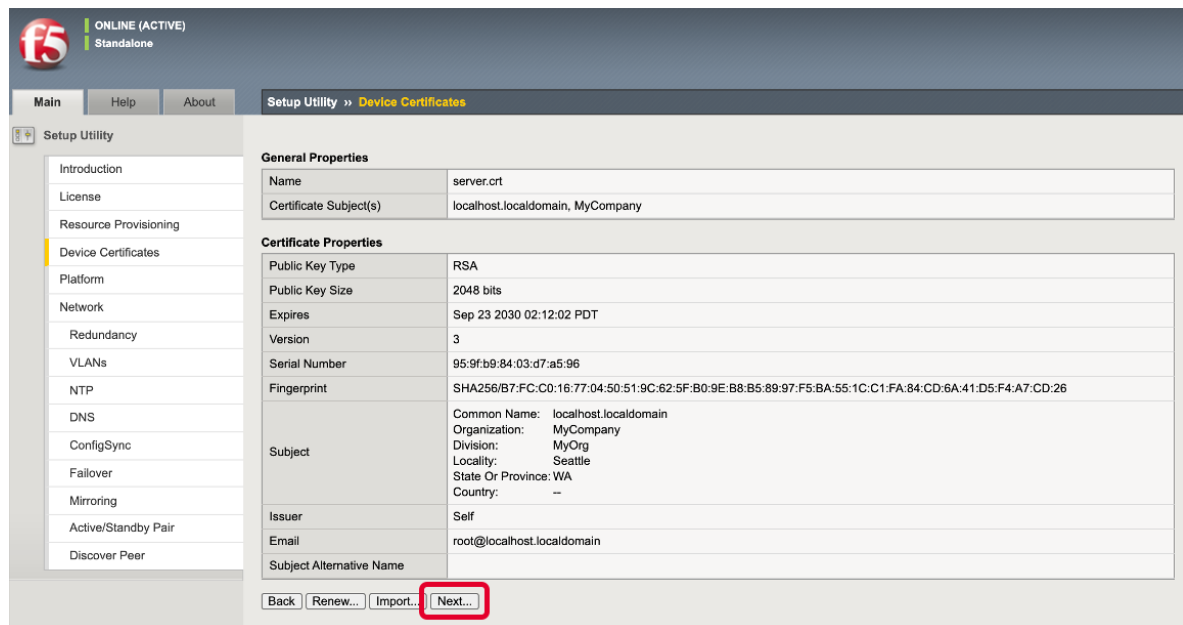
The screenshot shows the 'Setup Utility - Resource Provisioning' window. The left sidebar lists various setup steps, with 'Resource Provisioning' selected. The main area displays 'Modified Resource Allocation (prior to redistribution)' for CPU, Disk, and Memory. Below this is a table of modules with their provisioning status, license status, and resource requirements. The 'Application Security (ASM)' row is highlighted with a red rectangle. At the bottom, the 'Next...' button is also highlighted with a red rectangle.

Module	Provisioning	License Status	Required Disk (GB)	Required Memory (MB)
Management (MGMT)	Small	N/A	0	1264
Local Traffic (LTM)	<input type="checkbox"/> None	Unlicensed	0	1856
Application Security (ASM)	<input checked="" type="checkbox"/> Nominal	Licensed	20	1492
Fraud Protection Service (FPS)	<input type="checkbox"/> None	Licensed	12	544
Global Traffic (DNS)	<input type="checkbox"/> None	Unlicensed	0	148
Link Controller (LC)	<input type="checkbox"/> None	Unlicensed	0	148
Access Policy (APM)	<input type="checkbox"/> None	Limited mode available without a license	12	494
Application Visibility and Reporting (AVR)	<input type="checkbox"/> None	Licensed	16	576
Policy Enforcement (PEM)	<input type="checkbox"/> None	Unlicensed	16	1223
Advanced Firewall (AFM)	<input type="checkbox"/> None	Unlicensed	16	1058
Application Acceleration Manager (AAM)	<input type="checkbox"/> None	Unlicensed	32	2050
Secure Web Gateway (SWG)	<input type="checkbox"/> None	Unlicensed	24	4096
iRules Language Extensions (iRulesLX)	<input type="checkbox"/> None	Licensed	0	748
URLDB Minimal (URLDB)	<input type="checkbox"/> None	Unlicensed	36	2048
SSL Orchestrator (SSLO)	<input type="checkbox"/> None	Unlicensed	0	128
Carrier Grade NAT (CGNAT)	<input type="checkbox"/> None	Unlicensed	16	336

6. プロビジョニングには少し時間がかかります。終了したら、*Continue* ボタンを選択します。



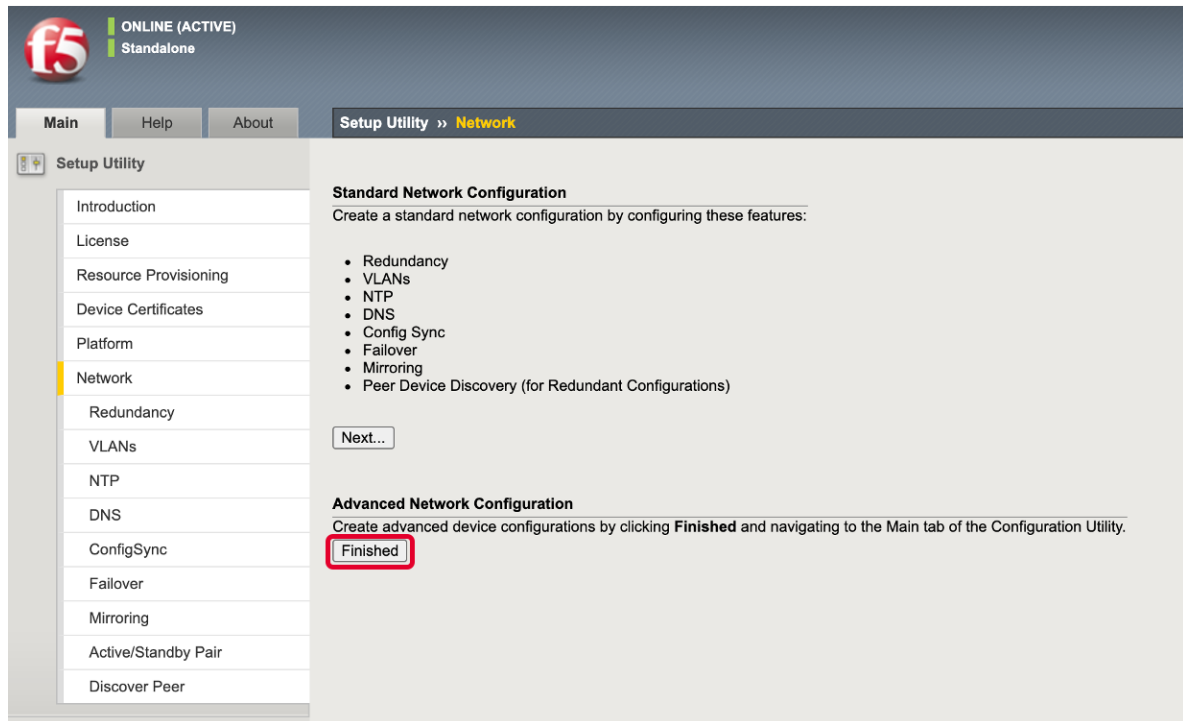
7. デバイス証明書の確認をし、*Next* ボタンを選択します。



8. **Host Name** に、**big80.f5jp.local** と設定し、**Time Zone** に **Japan** を選択し、**Root Account** のパスワードに **ilovef5** と記入し、**Next** ボタンを選択します。(F5 ハンズオントレーニング以外の場合は、それぞれの環境にあった内容を設定して下さい。)

The screenshot shows the F5 Setup Utility interface. At the top, there's a status bar indicating 'ONLINE (ACTIVE) Standalone' and 'Activation Complete'. The main navigation pane on the left lists various setup categories, with 'Platform' currently selected. The main content area is divided into two sections: 'General Properties' and 'User Administration'. In 'General Properties', the 'Host Name' is set to 'big80.f5jp.local' and the 'Time Zone' is set to 'Japan'. In 'User Administration', the 'Root Account' password and confirmation fields are both masked with asterisks. The 'SSH Access' checkbox is checked, and the 'SSH IP Allow' dropdown is set to '* All Addresses'. At the bottom of the configuration area, there are 'Back' and 'Next...' buttons, with the 'Next...' button being the focus of the instruction.

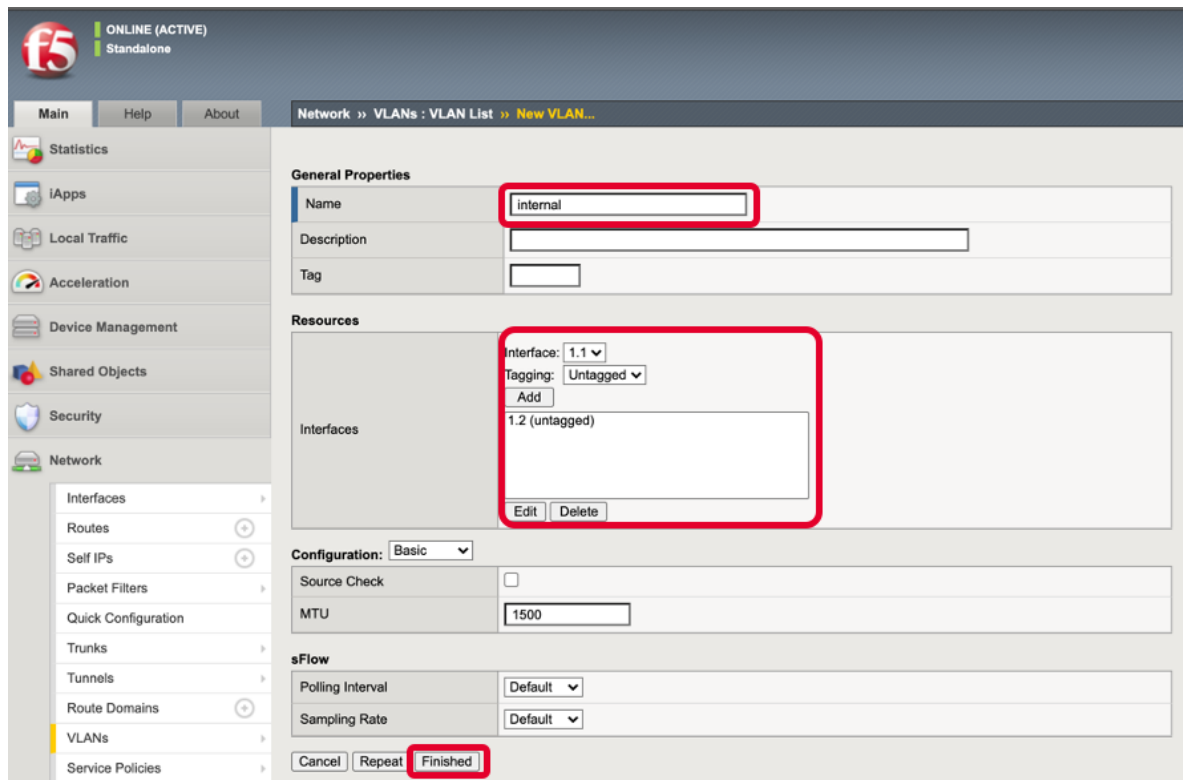
9. **Finished** ボタンを選択します。



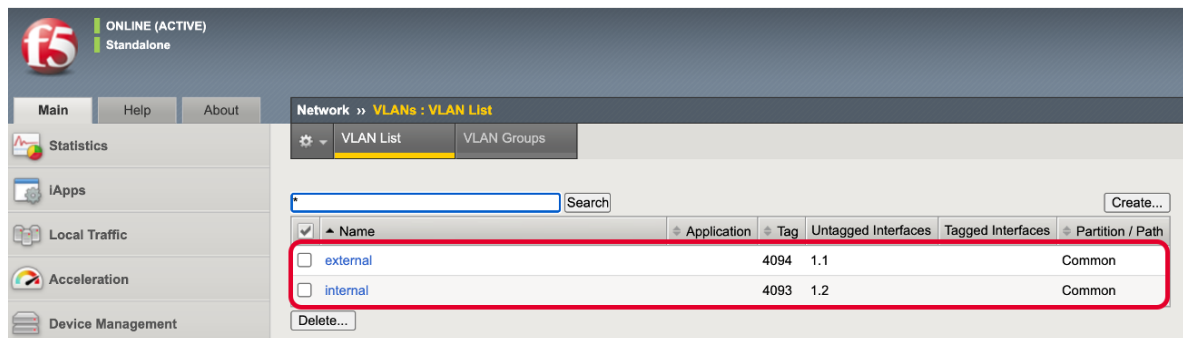
10. External VLAN の設定を行います。Network >> VLANs : VLAN List にて、Create ボタンを選択します。
Name に external と設定し、Interface に 1.1(Untagged) を選択し、Finished ボタンを選択します。

The screenshot shows the 'New VLAN' configuration page in the AWAF v17.1 web interface. The left sidebar contains a navigation menu with options like Statistics, IApps, Local Traffic, Acceleration, Device Management, Shared Objects, Security, and Network. The 'Network' section is expanded, showing a list of network-related items including Interfaces, Routes, Self IPs, Packet Filters, Quick Configuration, Trunks, Tunnels, Route Domains, VLANs, and Service Policies. The 'VLANs' item is selected, leading to the 'VLAN List' page. The 'New VLAN...' button is clicked, opening the configuration form. The form has several sections: 'General Properties' with fields for Name (set to 'external'), Description, and Tag; 'Resources' with a table for Interfaces (showing '1.1 (untagged)' and buttons for Add, Edit, and Delete); 'Configuration' with a dropdown for Basic and fields for Source Check and MTU (set to 1500); and 'sFlow' with dropdowns for Polling Interval and Sampling Rate. The 'Finished' button is highlighted with a red box.

11. Internal VLAN の設定を行います。Network >> VLANs : VLAN List にて、Create ボタンを選択します。
Name に internal と設定し、Interface に 1.2(Untagged) を選択し、Finished ボタンを選択します。



12. 以下のようになります。



13. External SelfIP の設定を行います。Network >> Self IP List にて、Create ボタンを選択します。Name に external-selfip と設定し、IP Address に 10.1.10.80、Netmask に 255.255.255. 0、VLAN/Tunnel に

external を選択し、**Port Lockdown** に **Allow None** を選択し、*Finished* ボタンを選択します。

ONLINE (ACTIVE)
Standalone

Main Help About Network >> Self IPs >> New Self IP...

Configuration

Name	external-selfip
IP Address	10.1.10.80
Netmask	255.255.255.0
VLAN / Tunnel	external
Port Lockdown	Allow None
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating)
Service Policy	None

Cancel Repeat **Finished**

14. Internal SelfIP の設定を行います。Network >> Self IP List にて、*Create* ボタンを選択します。Name に **internal-selfip** と設定し、IP Address に **10.1.20.80**、Netmask に **255.255.255.0**、VLAN/Tunnel に **internal** を選択し、Port Lockdown に **Allow Default** を選択し、*Finished* ボタンを選択します。

ONLINE (ACTIVE)
Standalone

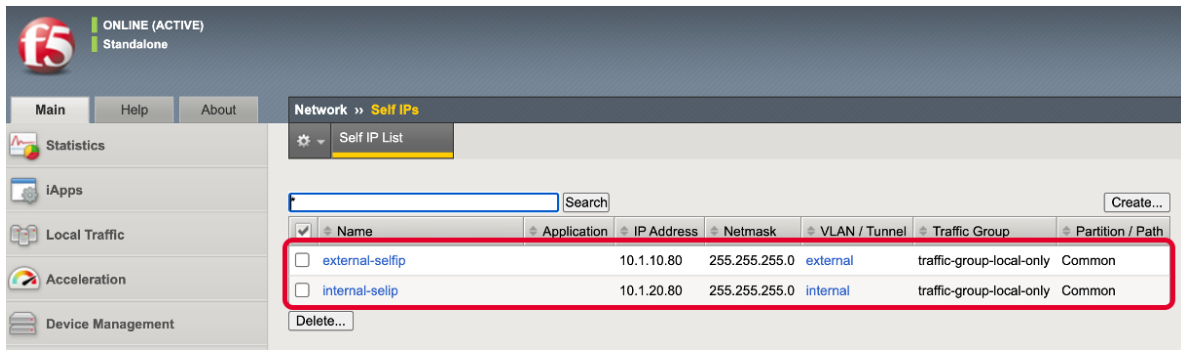
Main Help About Network >> Self IPs >> New Self IP...

Configuration

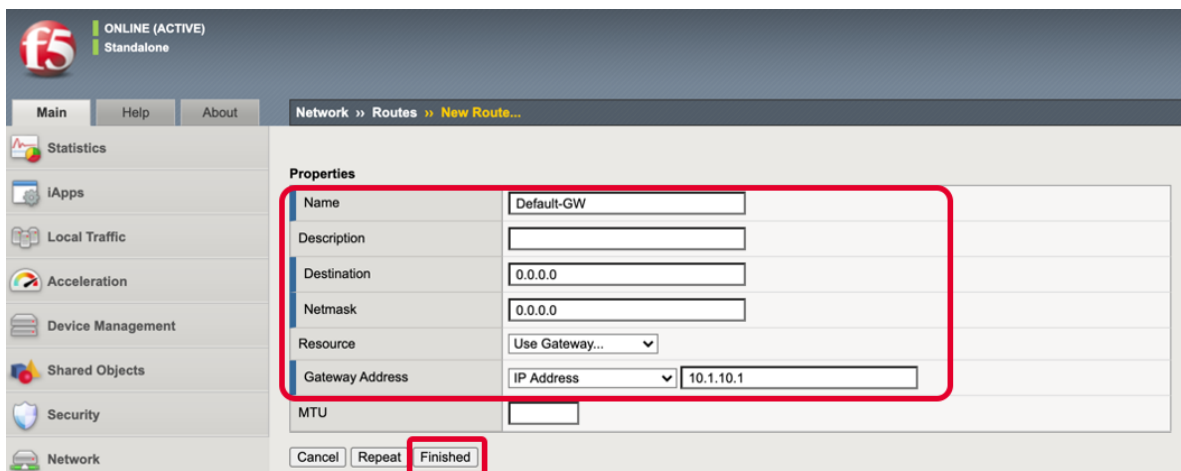
Name	internal-selfip
IP Address	10.1.20.80
Netmask	255.255.255.0
VLAN / Tunnel	internal
Port Lockdown	Allow Default
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating)
Service Policy	None

Cancel Repeat **Finished**

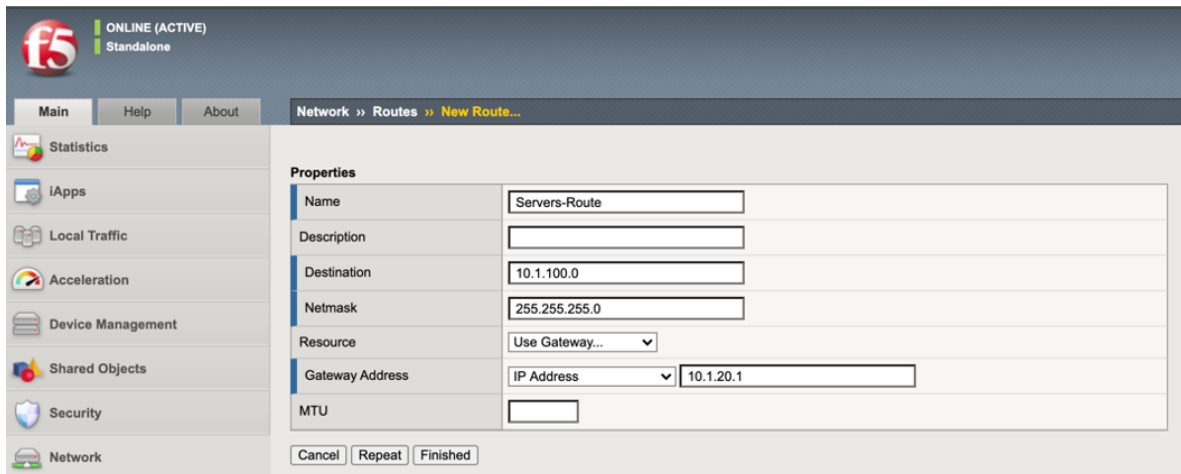
15. 以下のようになります。



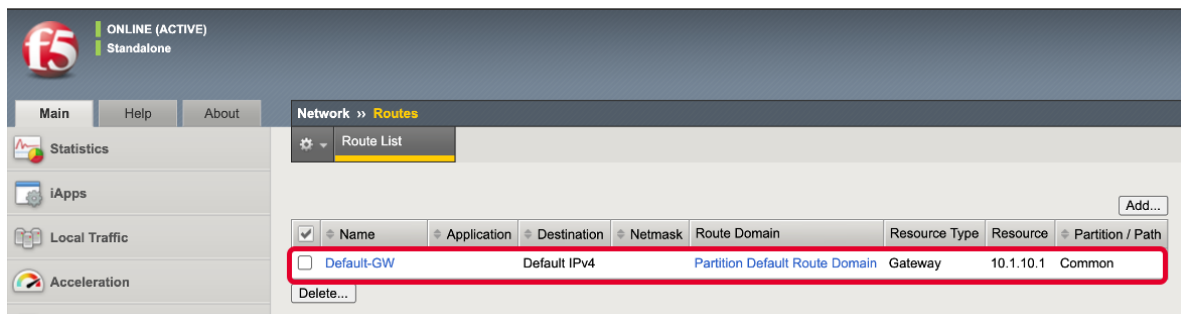
16. Default Gateway の設定を行います。Network >> Routes にて、Add ボタンを選択します。Name に任意の名前を設定し、Destination , Netmask に 0.0.0.0 を設定し、Gateway Address に 10.1.10.1 を設定し、Finished ボタンを選択します。



17. WEB サーバへのルーティング設定を行います。(以下は設定例となります。F5 ハンズオントレーニングでは、SelfIP と同じセグメントなため不要です。)



18. 以下のようになります。



19. DNS の設定を行います。**System >> Configuration : Device : DNS** にて設定します。F5 ハンズオントレーニングでは、10.1.1.2 を指定します。

The screenshot shows the 'System >> Configuration : Device : DNS' page. The 'Device' tab is selected. The 'Properties' section contains the following fields:

- DNS Lookup Server List:** A red box highlights the 'Address' field with the value '10.1.1.2'. Below it are 'Add', 'Edit', 'Delete', 'Up', and 'Down' buttons.
- BIND Forwarder Server List:** An empty 'Address' field with an 'Add' button and 'Edit', 'Delete', 'Up', 'Down' buttons below.
- DNS Search Domain List:** An empty 'Address' field with an 'Add' button and 'Edit', 'Delete', 'Up', 'Down' buttons below.
- DNS Cache:** A checkbox that is currently unchecked.
- IP Version:** A dropdown menu set to 'IPv4'.

An 'Update' button is located at the bottom left of the configuration area.

20. NTP の設定を行います。System >> Configuration : Device : NTP にて、NTP を設定し、*Update* ボタンを選択します。F5 ハンズオントレーニングでは NICT の NTP を利用します。

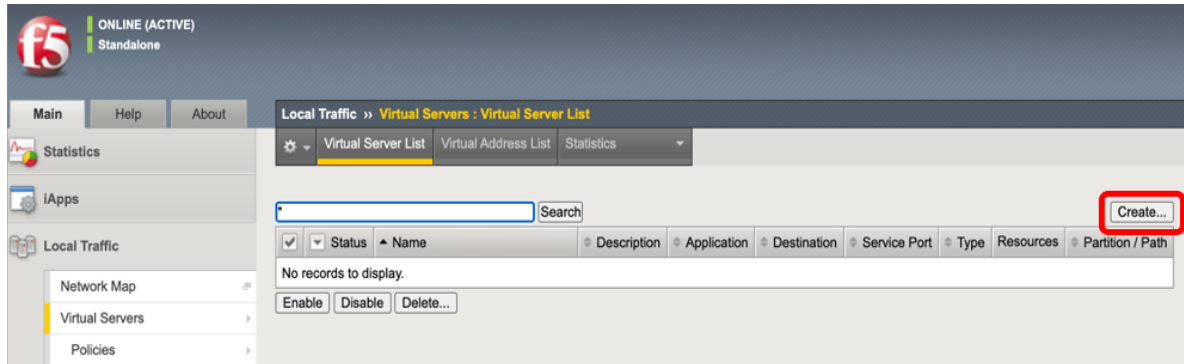
The screenshot shows the 'System >> Configuration : Device : NTP' page. The 'Device' tab is selected. The 'Properties' section contains the following fields:

- Time Server List:** A red box highlights the 'Address' field with the value 'ntp.nict.jp'. Below it are 'Add', 'Edit', and 'Delete' buttons.

An 'Update' button is located at the bottom left of the configuration area.

2.1.4 （脆弱な）WEB サーバの登録

1. Virtual Server を作成します。Local Traffic >> Virtual Servers : Virtual Server List にて、*Create* ボタンを押します。



2. Name に任意の名称を記述し、Destination Address/Mask に 10.1.10.180、Service Port に 443 を設定し、HTTP Profile (Client) にて HTTP を選択、SSL Profile(Client) にて clientssl を選択します。

ONLINE (ACTIVE)
Standalone

Main Help About

Local Traffic » Virtual Servers : Virtual Server List » New Virtual Server...

Statistics
IApps
Local Traffic
Network Map
Virtual Servers
Policies
Profiles
Ciphers
IRules
Pools
Nodes
Monitors
Traffic Class
Address Translation
Acceleration
Device Management
Shared Objects
Security
Network
System

General Properties

Name: DVWA_HTTPS_VIP

Description:

Type: Standard

Source Address: Host Address List

Destination Address/Mask: Host Address List 10.1.10.180

Service Port: Port 443 HTTPS

Notify Status to Virtual Address: ☒

State: Enabled

Configuration: Basic

Protocol: TCP

Protocol Profile (Client): tcp

Protocol Profile (Server): (Use Client Profile)

HTTP Profile (Client): http

HTTP Profile (Server): (Use Client Profile)

HTTP Proxy Connect Profile: None

FTP Profile: None

PPTP Profile: None

SSL Profile (Client): /Common clientssl

Available: /Common clientssl-insecure-compatible, clientssl-quick, clientssl-secure, crypto-server-default-clientssl, split-session-default-clientssl, wom-default-clientssl

3. Source Address Translation にて、Automap を選択します。

Service Profile: None

SMTP Profile: None

VLAN and Tunnel Traffic: All VLANs and Tunnels

Source Address Translation: Auto Map

Content Rewrite

Rewrite Profile: + None

4. Default Pool にて、+ ボタンを選択します。

Default Pool	+ None ▼
Default Persistence Profile	None ▼
Fallback Persistence Profile	None ▼

5. Pool を作成します。Name にて、任意の名称を入力し、Health Monitors にて **gateway_icmp** を選択し、New Members に、WEB サーバ (Address : 10.1.20.202, Service Port : 80) を加えて Add ボタンを押し、Finished ボタンを押します。

Configuration: Basic ▼

Name: DVWA_HTTP_Pool

Description:

Health Monitors:

Active: gateway_icmp

Available: http, http2, http2_head_f5, http_head_f5

Resources:

Load Balancing Method: Round Robin

Priority Group Activation: Disabled

New Members:

Node Name	Address/FQDN	Service Port	Auto Populate	Priority
10.1.20.202	10.1.20.202	80		0

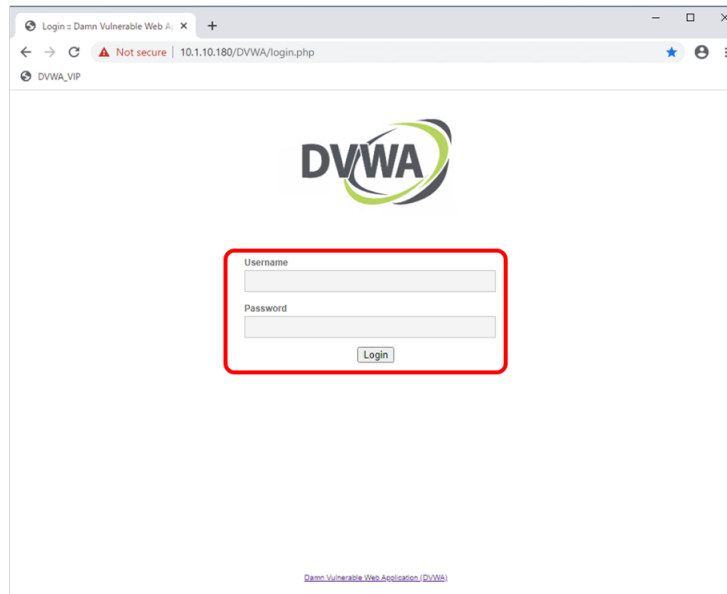
Cancel Finished

6. Default Pool に Pool が追加されたことを確認し、Finished ボタンを押します。

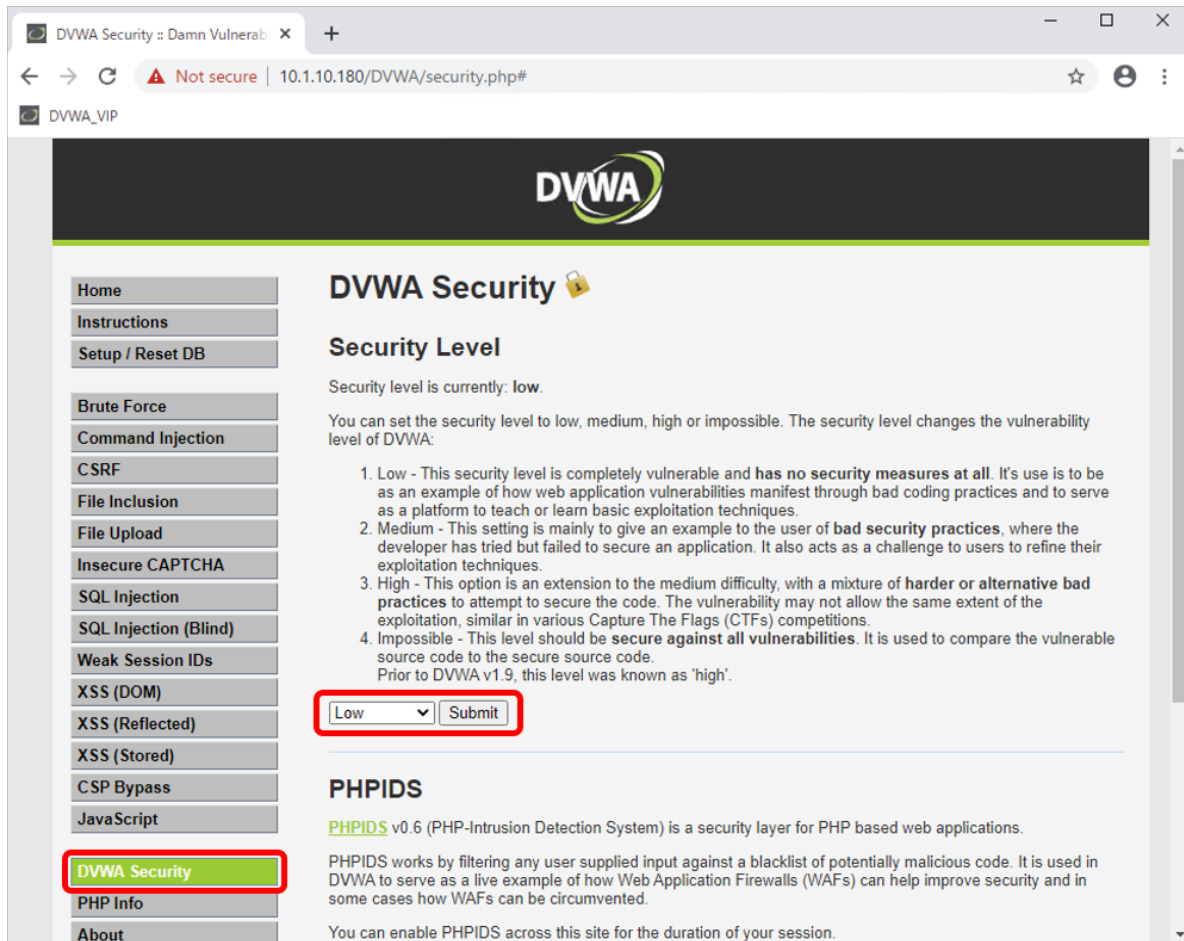
Default Pool	+ DVWA_HTTP_Pool ▼
Default Persistence Profile	None ▼
Fallback Persistence Profile	None ▼

Cancel Repeat Finished

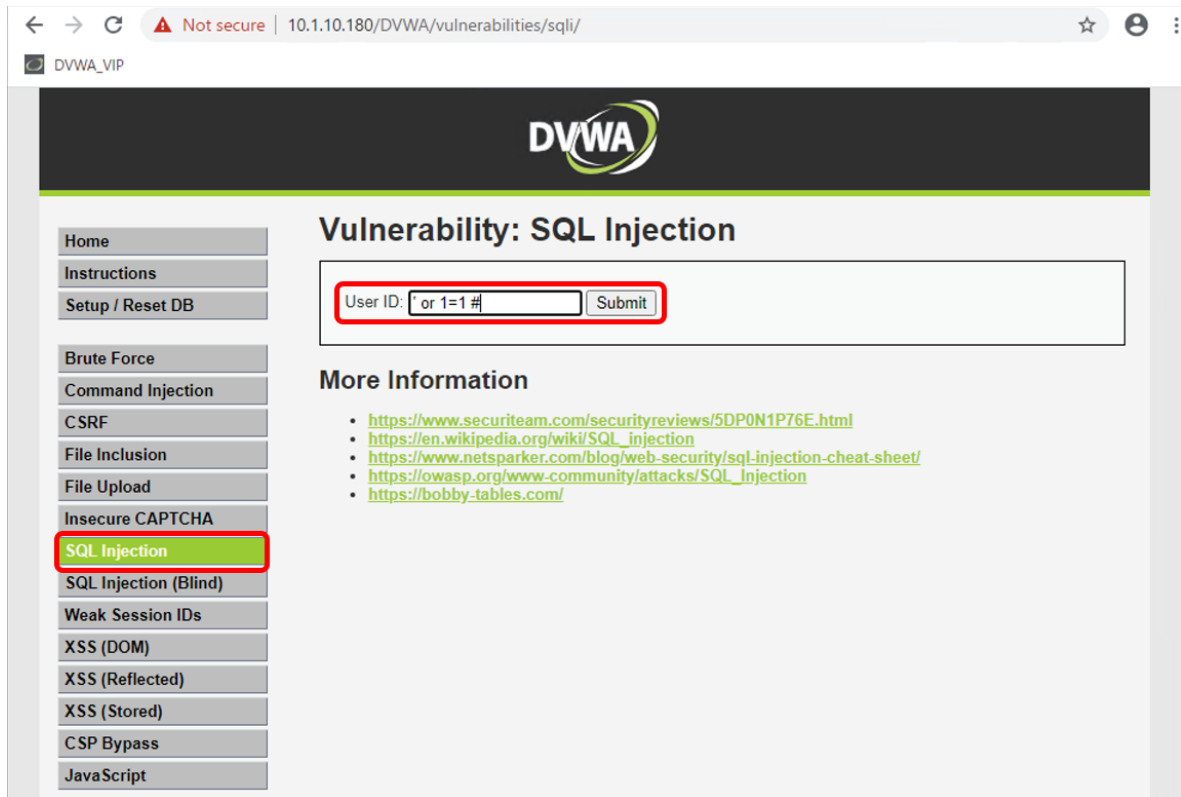
7. Windows クライアントを起動し、<https://10.1.10.180/DVWA/login.php> にアクセスします。Username: **admin**、Password: **password** でログインします。



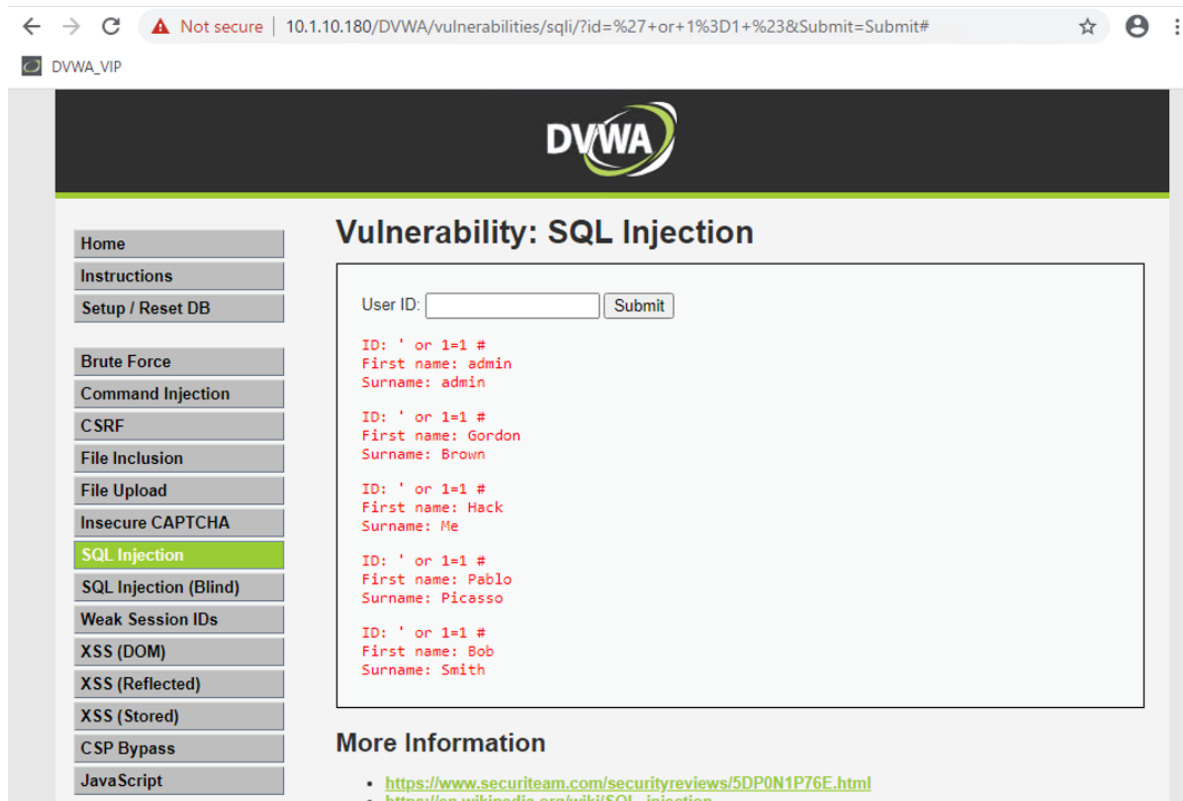
8. DVWA Security にアクセスし、Security Level を Low に設定します。



9. 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。)

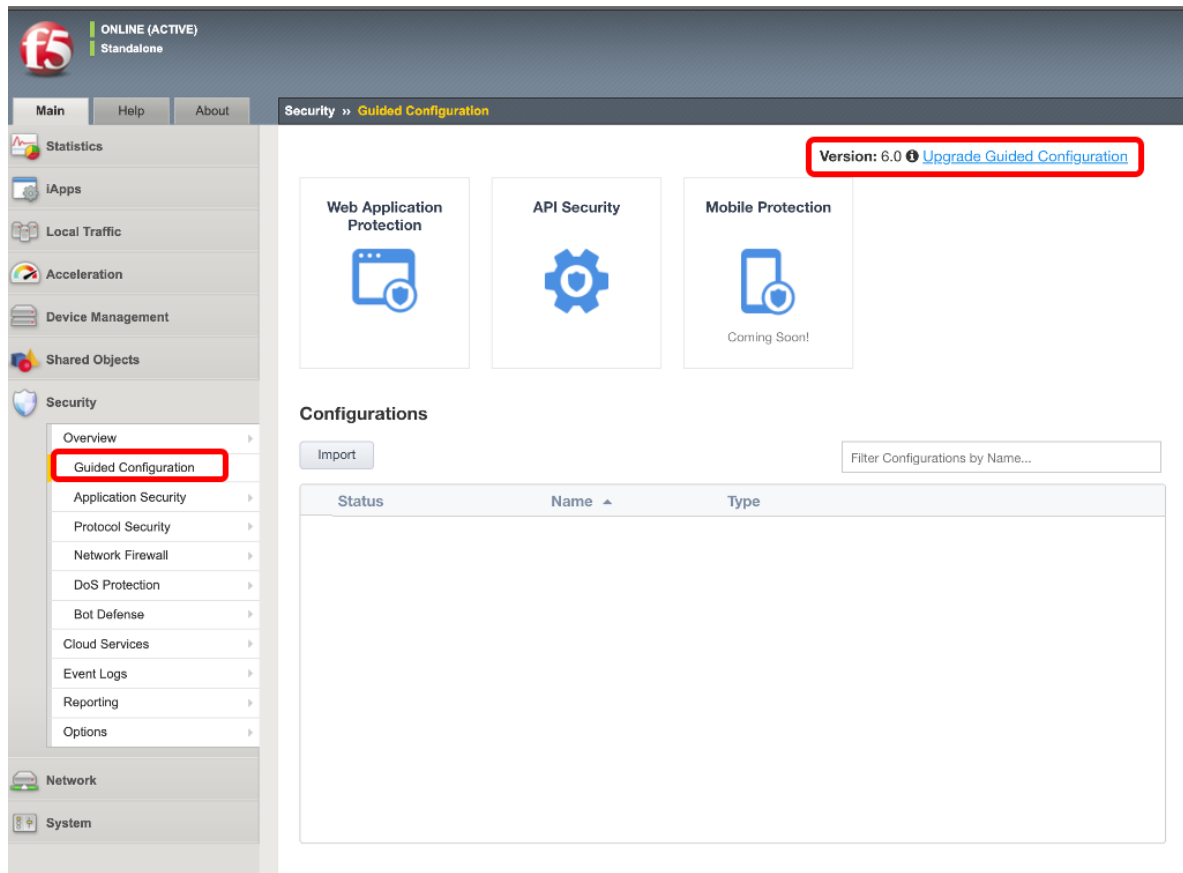


10. SQL インジェクション攻撃が成功し、User ID が複数表示されることを確認します。



2.1.5 Guided configuration による WAF ポリシーの作成

1. **Security >> Guided Configuration**を開きます。Guided Configuration のバージョンを確認します。(Guided Configuration の起動には少し時間がかかります。)



2. [MyF5 の Download サイト](#) にて、最新版の Guided Configuration をダウンロードします。ダウンロードには MyF5 のアカウント登録が必要となります。アカウント登録は数分で行うことはできますが、F5 ハンズオン受講者でアカウントをすぐに作成することができない方は、Windows Client デスクトップ上のダウンロード済みのファイルをご利用下さい。（既に最新版をご利用の場合は、アップデート作業は不要なので、手順 7 に進んで下さい。）

Downloads

Select a product family

Group

BIG-IP

Tell us more about your product

Product Line

Guided Configuration

Product Version

10.0

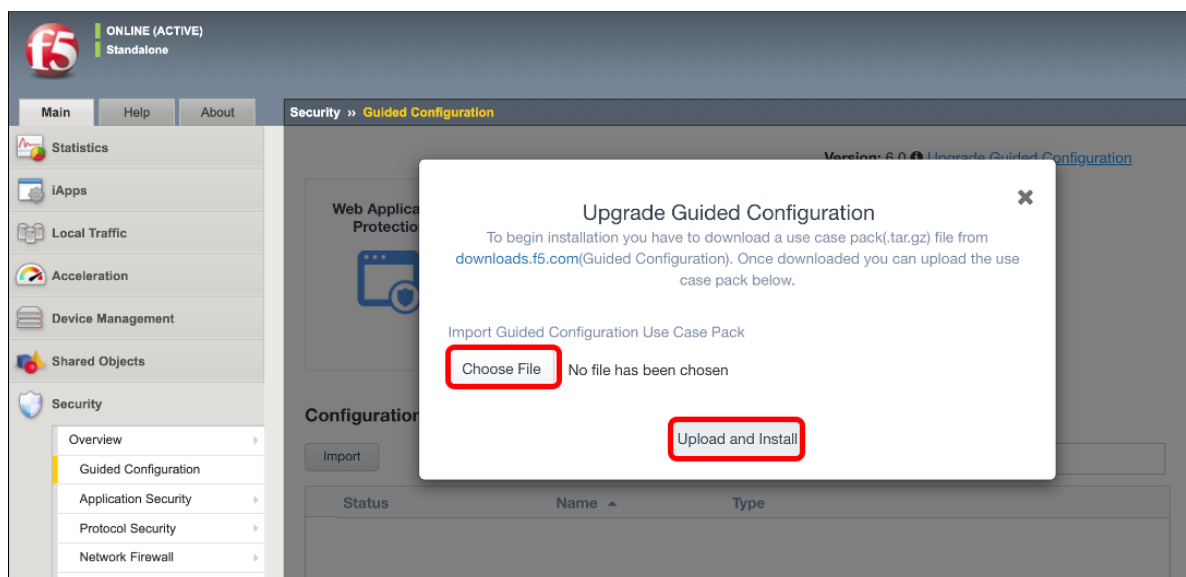
Select a product container

Name ↑↓	Type ↑↓	Date ↑↓	Description ↑↓
<input checked="" type="radio"/> Guided_Configuration	Release	Mar 15, 2023	Guided_Configuration

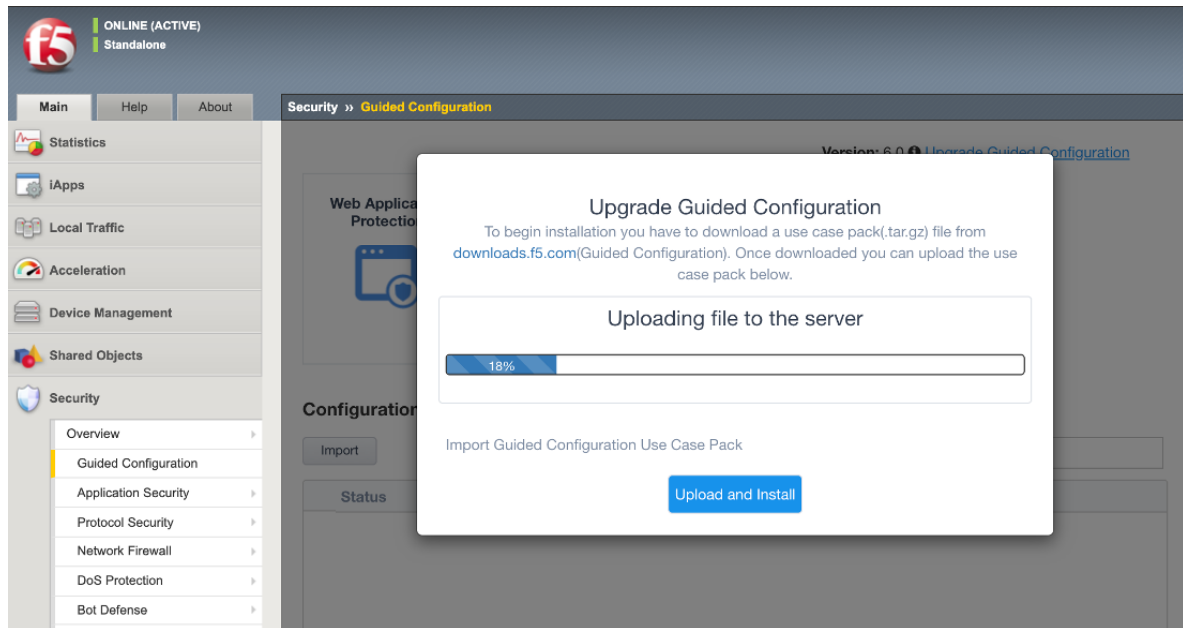
Select a download file

File Name ↑↓	Description	Size
<input checked="" type="radio"/> f5-lappslx-agc-usecase-pack-10.0-0.0.1636.tar.gz	Access and Advanced WAF Guided Configuration 10.0	10 MB
<input type="radio"/> f5-lappslx-agc-usecase-pack-10.0-0.0.1636.tar.gz.md5	MD5 file for Access and Advanced WAF Guided Configuration 10.0	82 Bytes
<input type="radio"/> relnote-guided-config-10-0.html	Guided Configuration 10.0 release note	86 KB
<input type="radio"/> relnote-guided-config-10-0.html.md5	Guided Configuration 10.0 release note	66 Bytes

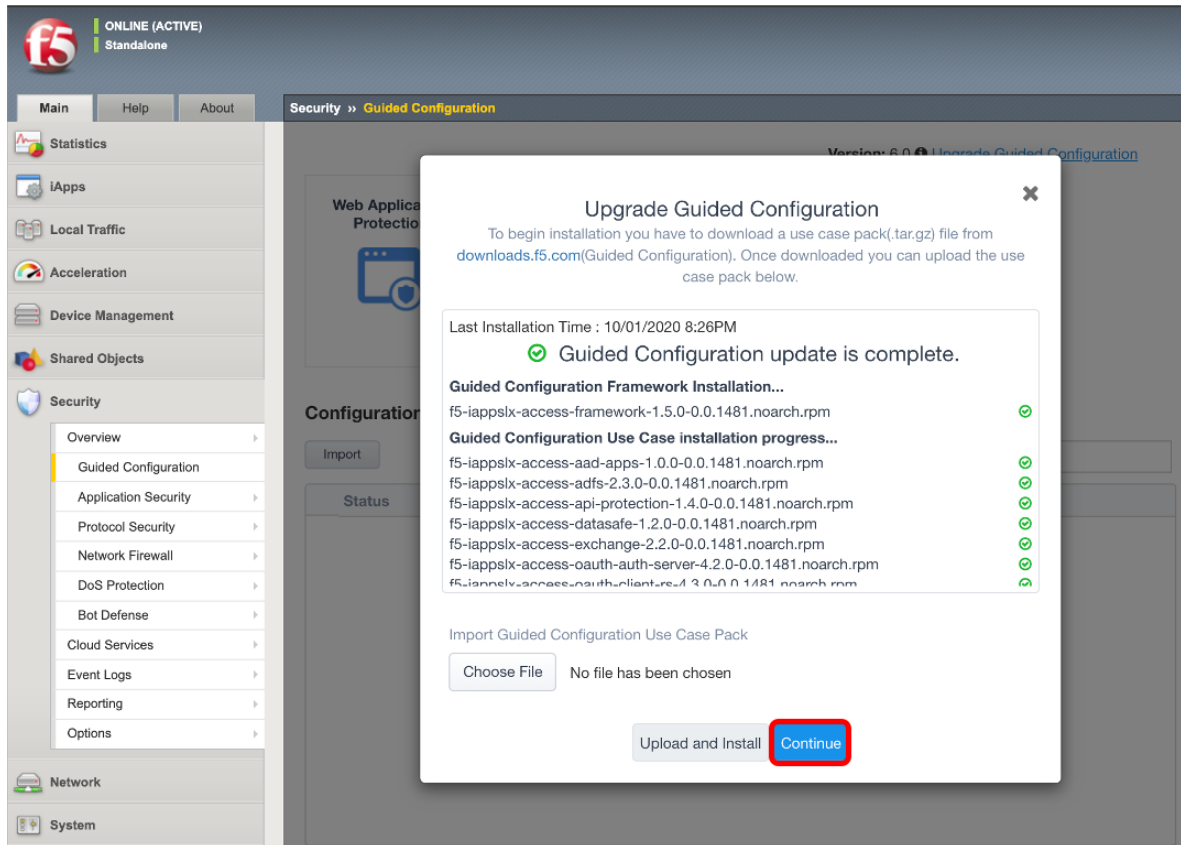
- AWAF の先程の画面に戻り、右上の **Upgrade Guided Configuration** をクリックし、ダウンロードした Guided Configuration ファイル (xxx.tar.gz) をアップロード、インストールします。



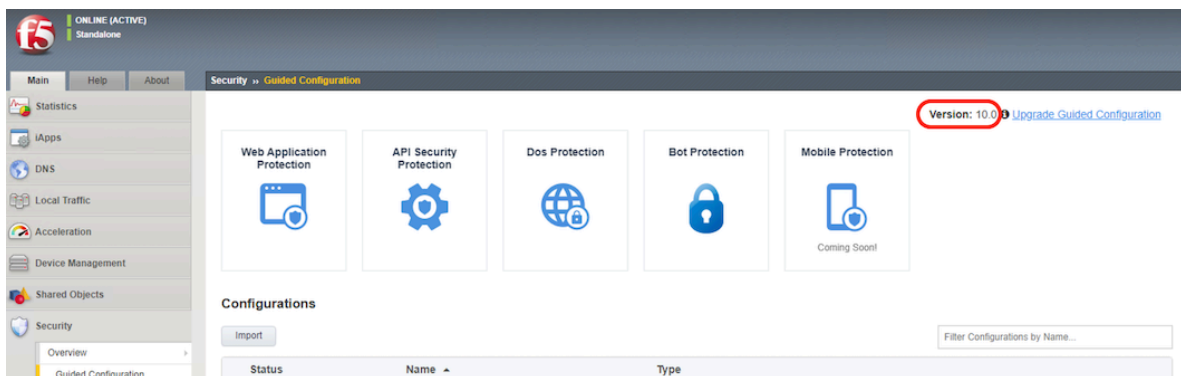
4. インストールしている途中のイメージです。



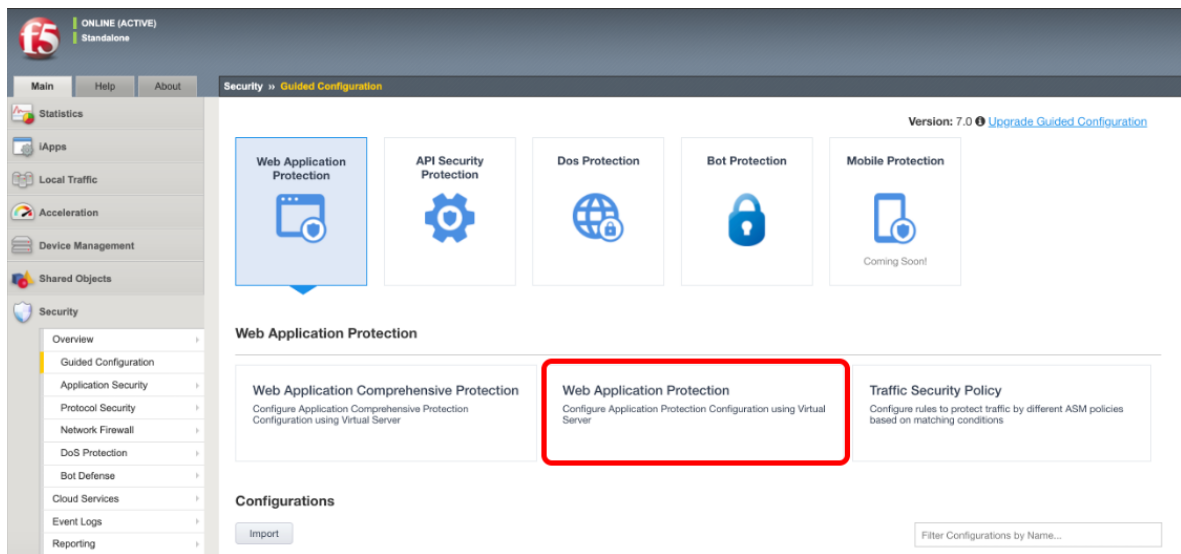
5. インストールが終了したら、*Continue* ボタンを押します。



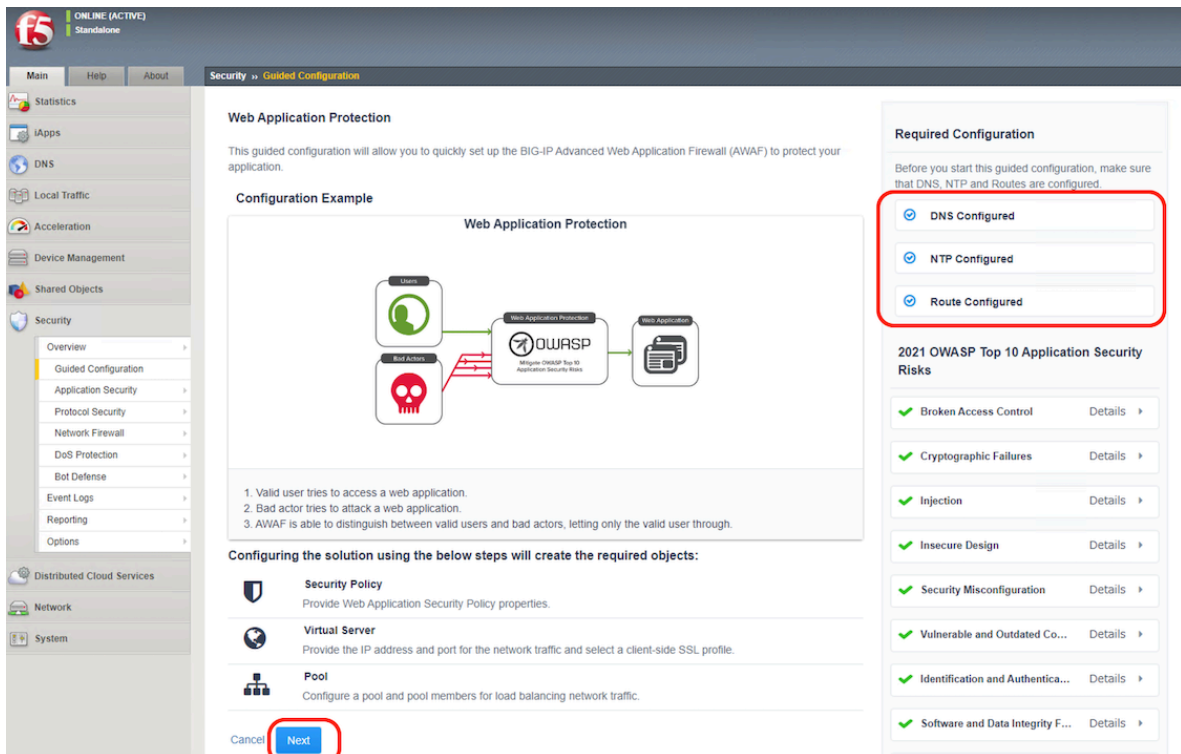
6. Guided Configuration のバージョンがアップデートされていることを確認します。



7. Web Application Protection の Web Application Protection を選択します。



8. DNS, NTP, Routing が設定 OK となっていることを確認し、Next ボタンを押します。



9. 右上の **Show Advanced Setting** をクリックし、**Security Policy Name** に任意の名前を設定し、**Enforcement Mode** にて **Transparent** を選択し、**type of policy to protect application** にて、**Generic** を選択し、**Server Technologies** にて利用しているミドルウェアや言語を選択します。F5 ハンズオン環境では、**Apache**, **MySQL**, **PHP** を選択し、**Next** ボタンを押します。

Security » Guided Configuration

Web Application Protection Configuration NOT SAVED

Security Policy Virtual Server Summary

Web Application Security Policy Properties

[Hide Advanced Setting](#)

Security Policy Name
DVWA_policy

Select Enforcement Mode ⓘ
☒ Transparent ☐ Blocking

Select type of policy to protect application ⓘ
☒ Generic ☐ Application Specific

Application Language ⓘ
Unicode (utf-8)

Server Technologies ⓘ

Available	Selected
Filter	
AngularJS	Apache/NCSA HTTP Server
Apache Struts	MySQL
Apache Tomcat	PHP

☐ Trust XFF Headers ⓘ

Cancel Save Draft **Save & Next**

10. 既に Virtual Server は作成済みなので、ここでは、**Assign Policy to Virtual Server(s)** にチェックを入れ、**Use Existing** を選択し、作成済みの Virtual Server を右に移動させ、**Save & Next** ボタンを押します。

Security » Guided Configuration

Web Application Protection Configuration :DVWA_policy NOT DEPLOYED

Security Policy Virtual Server Summary

Virtual Server Properties

☒ Assign Policy to Virtual Server(s)

Virtual Server

☐ Create New ☒ Use Existing

Assign Virtual Servers

Available

Filter

No available items

Selected

/Common/DVWA_HTTPS_VIP

Cancel Save Draft Back Save & Next


11. 内容を確認し、*Deploy* ボタンを押します。

Security >> Guided Configuration

Web Application Protection Configuration : DVWA_policy NOT DEPLOYED

Security Policy Virtual Server Summary

Your application is ready to be deployed.

The application is correctly configured, and ready to be deployed. Review the summary. You can click  on any step to make changes.

Summary

Security Policy ▾	
Security Policy Name	DVWA_policy
Type of policy to protect application	Generic
Enforcement Mode	Transparent
Application Language	Unicode (utf-8)
Server Technologies	Apache/NCSA HTTP Server, MySQL, PHP
Trust XFF Headers	Disabled

Virtual Server ▸	
------------------	--

Cancel Save Draft Back **Deploy**

12. 作成した WAF のポリシーに Logging Profile をアタッチします。Security >> Overview:Summary にて、作成済みの Virtual Server を選択し、Attach の Logging Profile を選択します。

ONLINE (ACTIVE)
Standards
Live Updates Available

Main Help About

Statistics
iApps
Local Traffic
Acceleration
Device Management
Shared Objects
Security
Overview
Guided Configuration

Security >> Overview:Summary

Summary Analytics Application Protocol DoS OWASP Compliance Dashboard




Attach Detach Create

Blocking Transparent Disabled Detached

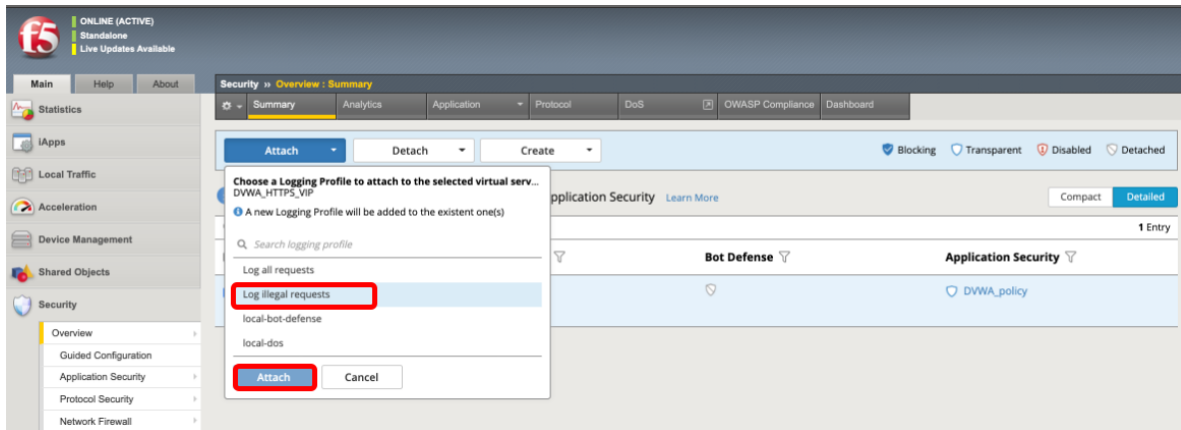
DoS Protection → Bot Defense → Application Security [Learn More](#)

Compact Detailed

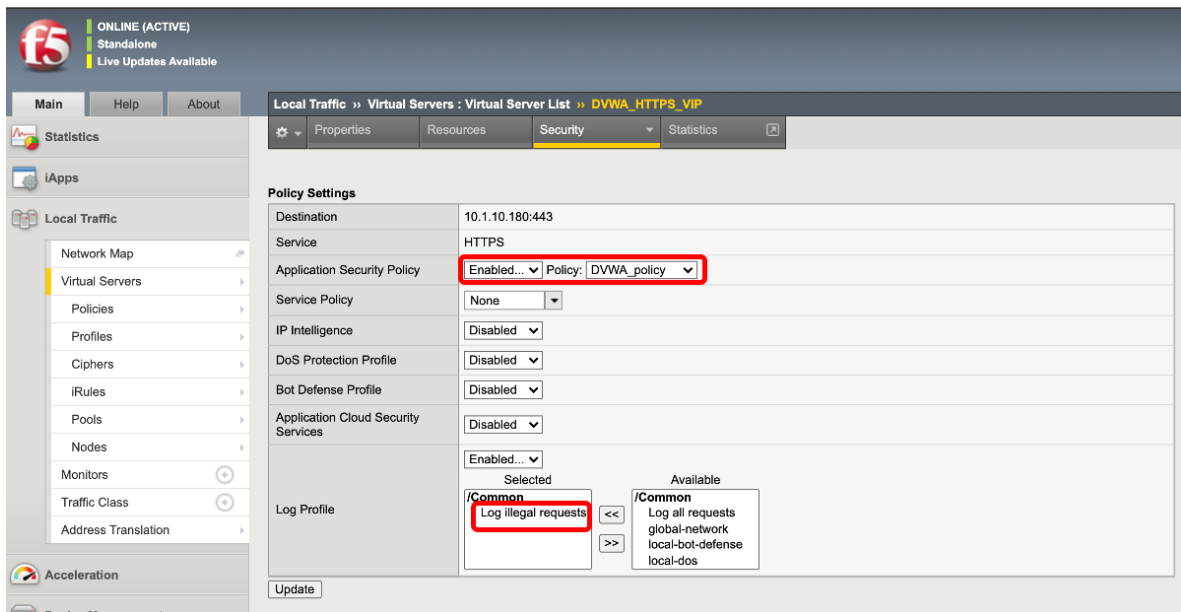
Profiles and policies 1 Entry

	DoS Protection ▾	Bot Defense ▾	Application Security ▾
<input checked="" type="checkbox"/> DVWA_HTTPS_VIP			 DVWA_policy

13. Log illegal requests を選択し、Attach ボタンを押します。

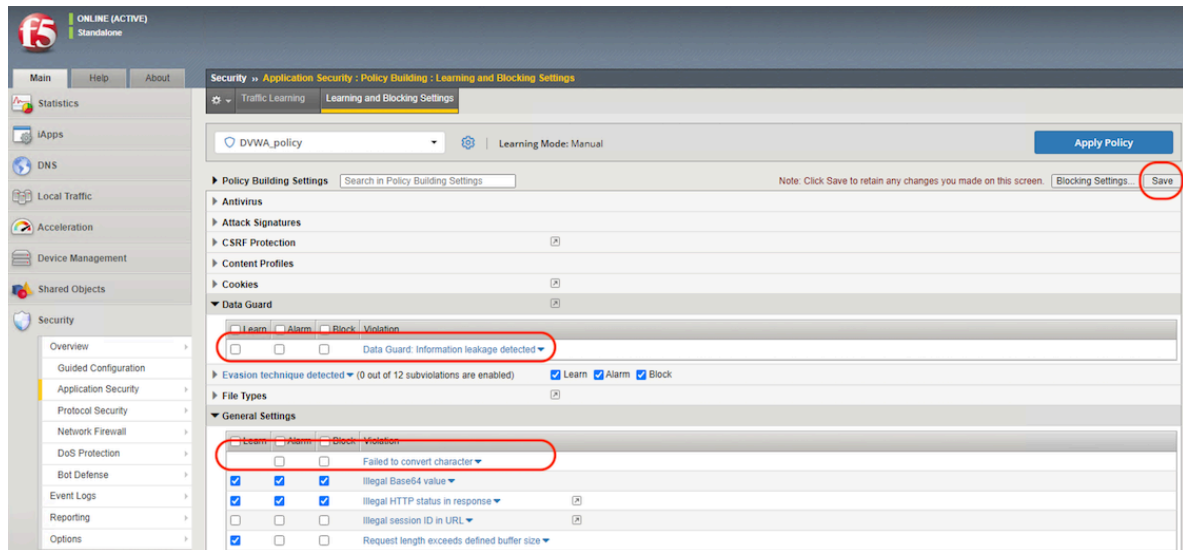


14. **Local Traffic >> Virtual Servers:Virtual Server List** にて作成済みの Virtual Server を選択し、**Security** タブの **Policies** を選択します。Application Security Policy と Log Profile がそれぞれ設定されていることを確認します。

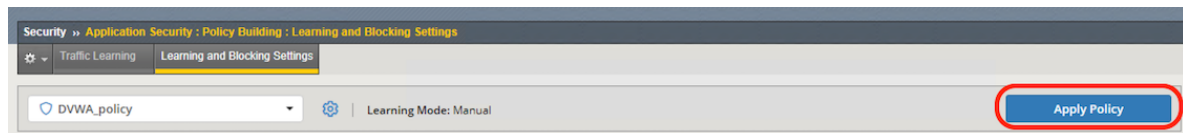


15. 次に誤検知対策、負荷防止対策を設定します。(必須ではありません。) **Security >> Application Security : Policy Building : Learning and Blocking Settings** を開きます。日本語サイトの誤検知の防止策とし

て、**Failed to convert character** を OFF にします。また、**Data Guard:Information Leakage Detected** もパフォーマンス面を考慮して OFF にし、**Save** ボタンを押します。

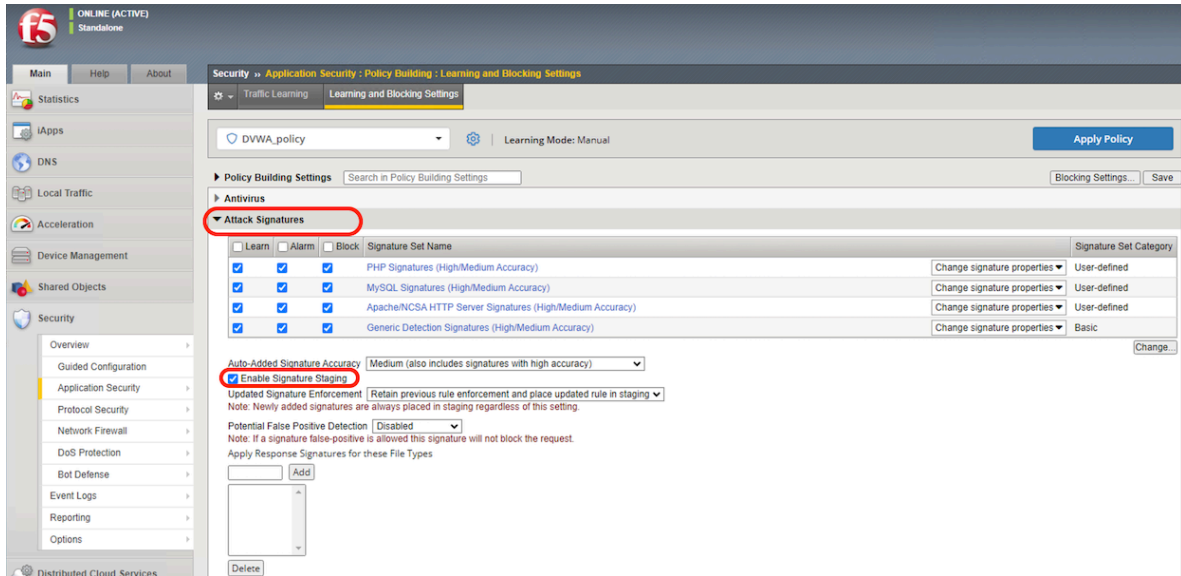


16. **Apply Policy** ボタンを押し、ポリシーを反映させます。

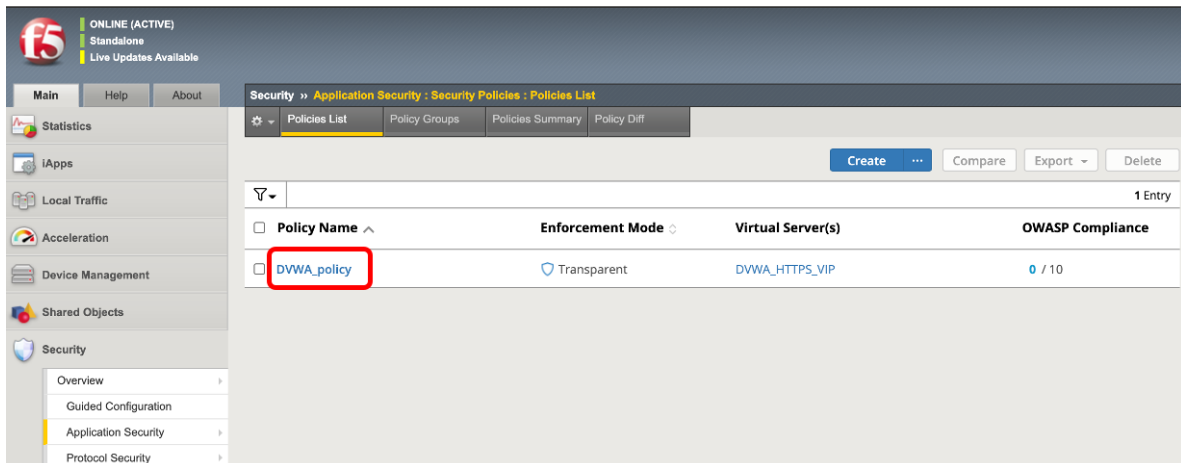


2.1.6 シグネチャの状態確認

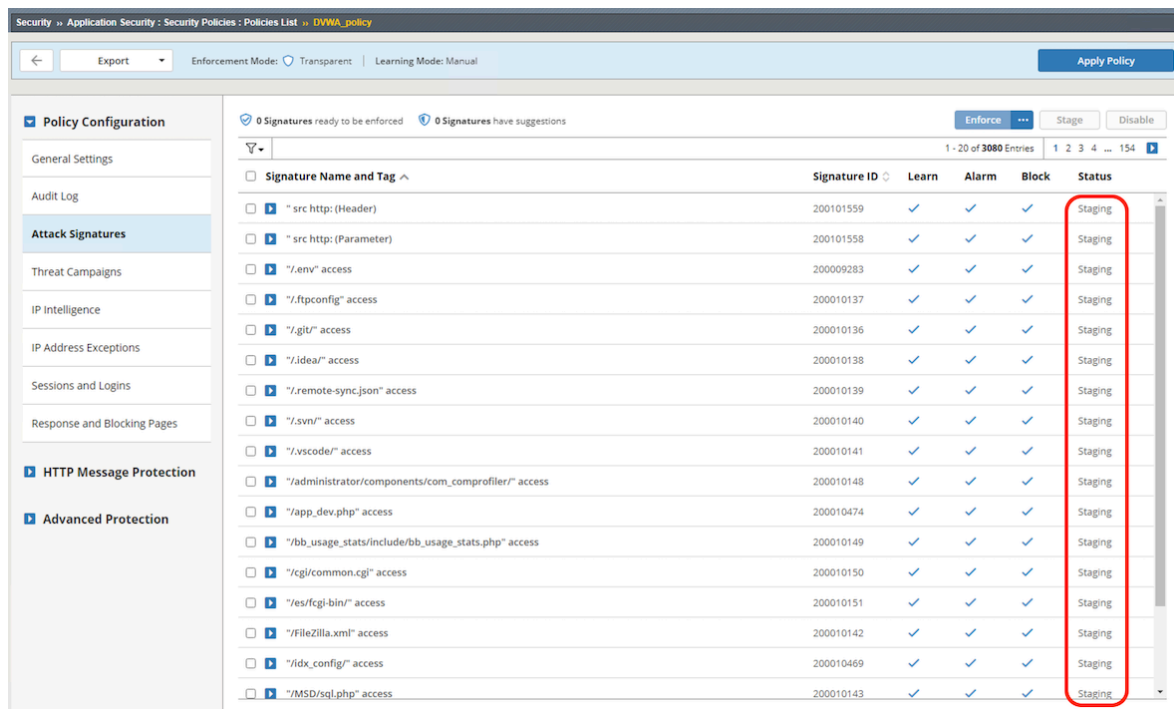
1. **Security >> Application Security : Policy Building : Learning and Blocking Settings** を開きます。**Attack Signatures** のところで、**Enable Signature Staging** にチェックが入っていることを確認します。



2. **Security >> Application Security : Security Policies : Policies List** を開きます。作成済みのセキュリティポリシーをクリックします。



3. **Attack Signatures** をクリックします。作成済みのセキュリティポリシーをクリックします。シグネチャのステータスが **Staging** となっていることを確認します。

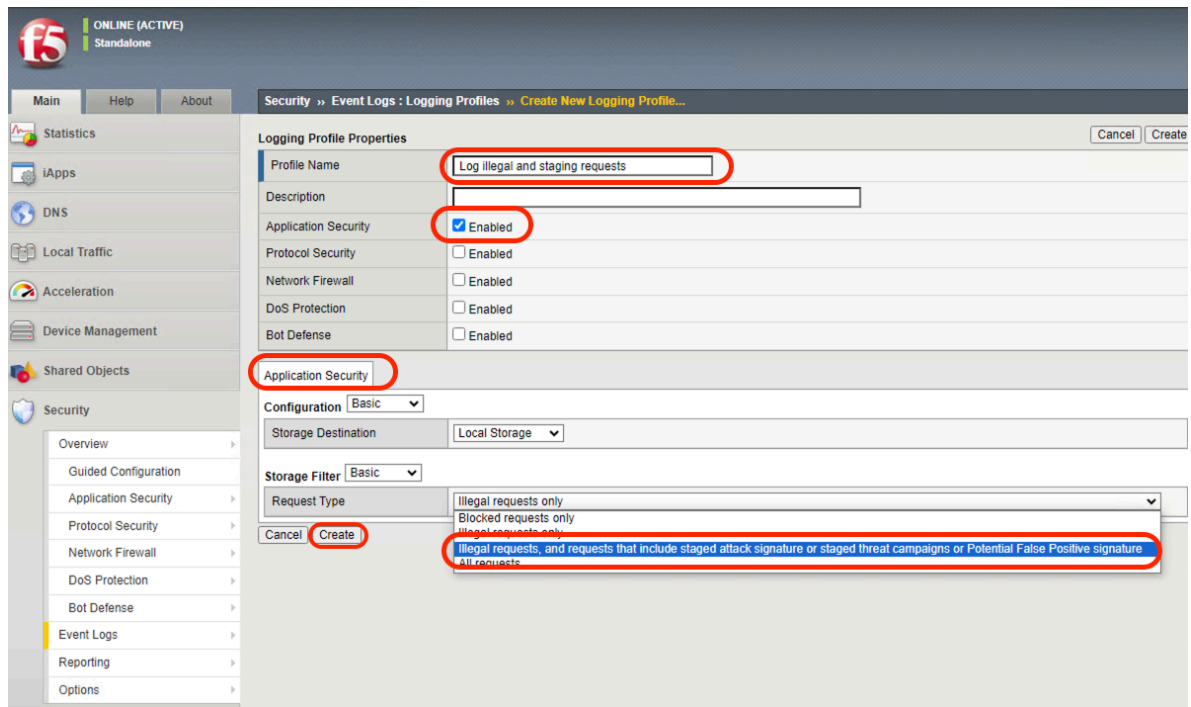


注釈: Staging(ステージング) モードとは、Block 設定が無効化され、攻撃を検知した場合には、「Manual Traffic Learning」で学習するだけの動作となるモードです。

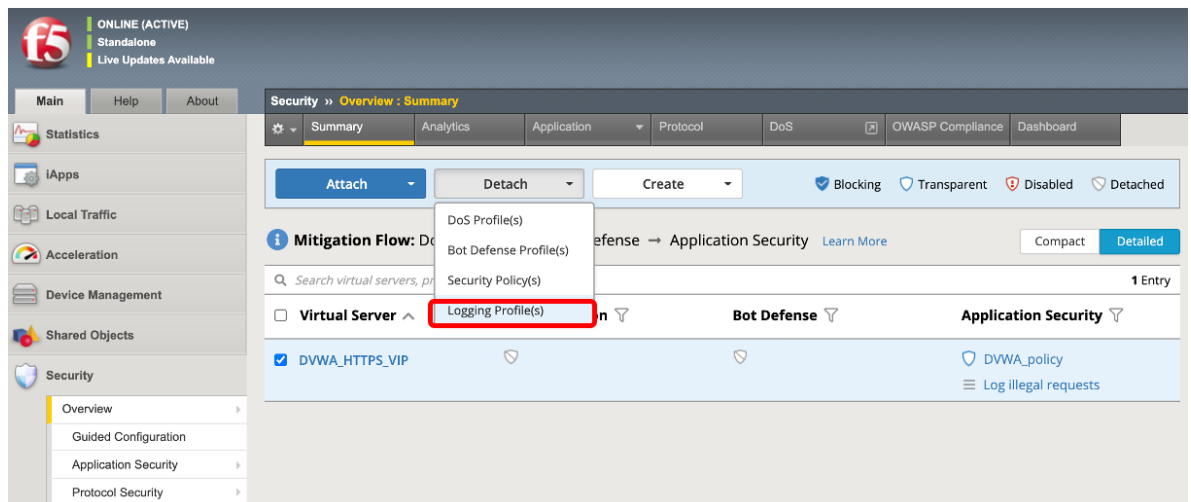
2.1.7 ステージングログの設定

ステージングのログを Event Logs に出力するための設定を行います。(必須ではありませんが、ステージング運用される場合には便利です。)

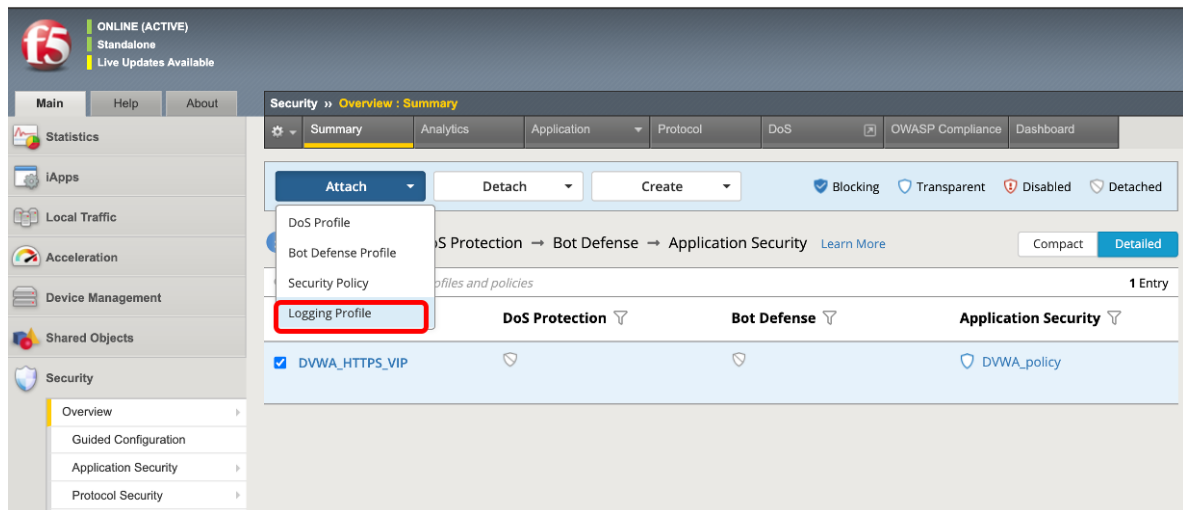
1. **Security >> Event Logs : Logging Profiles** にて、**Create** ボタンを押します。任意の名前を設定し、**Application Security** のところで、**Enabled** をチェックし、**Request type** にて、**Illegal requests, and requests that include staged attack signatures or staged threat campaigns or Potential False Positive signature ...** を選択し、**Create** ボタンを押します。



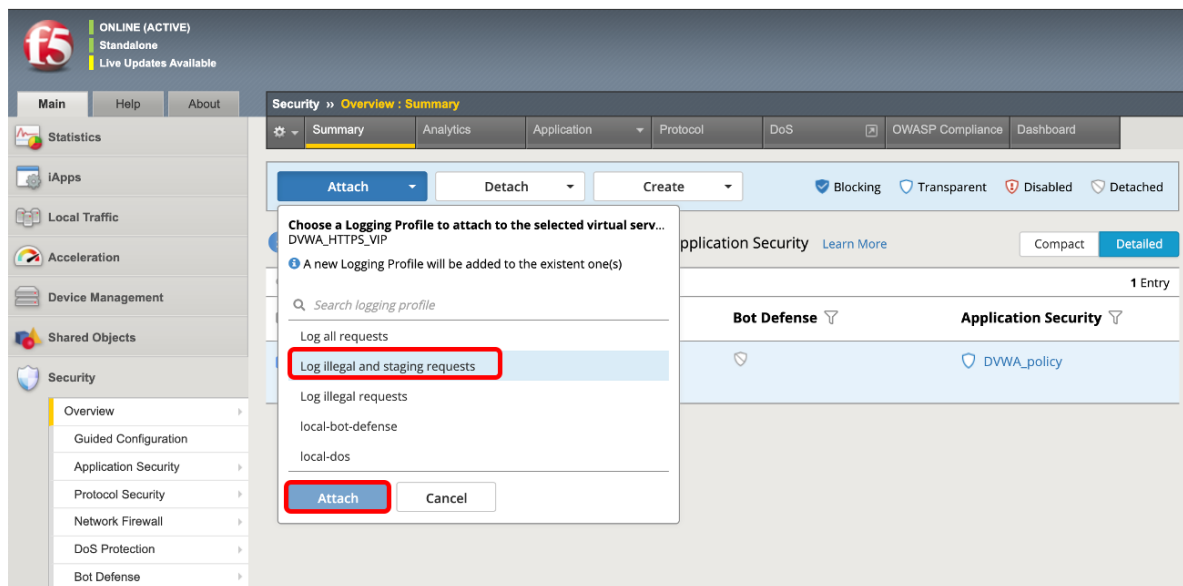
2. **Security >> Overview : Summary** にて、作成済みの Virtual Server にチェックをし、一旦、アタッチした **Logging Profile(s)** をはずします。



3. 再度アタッチの設定をします。

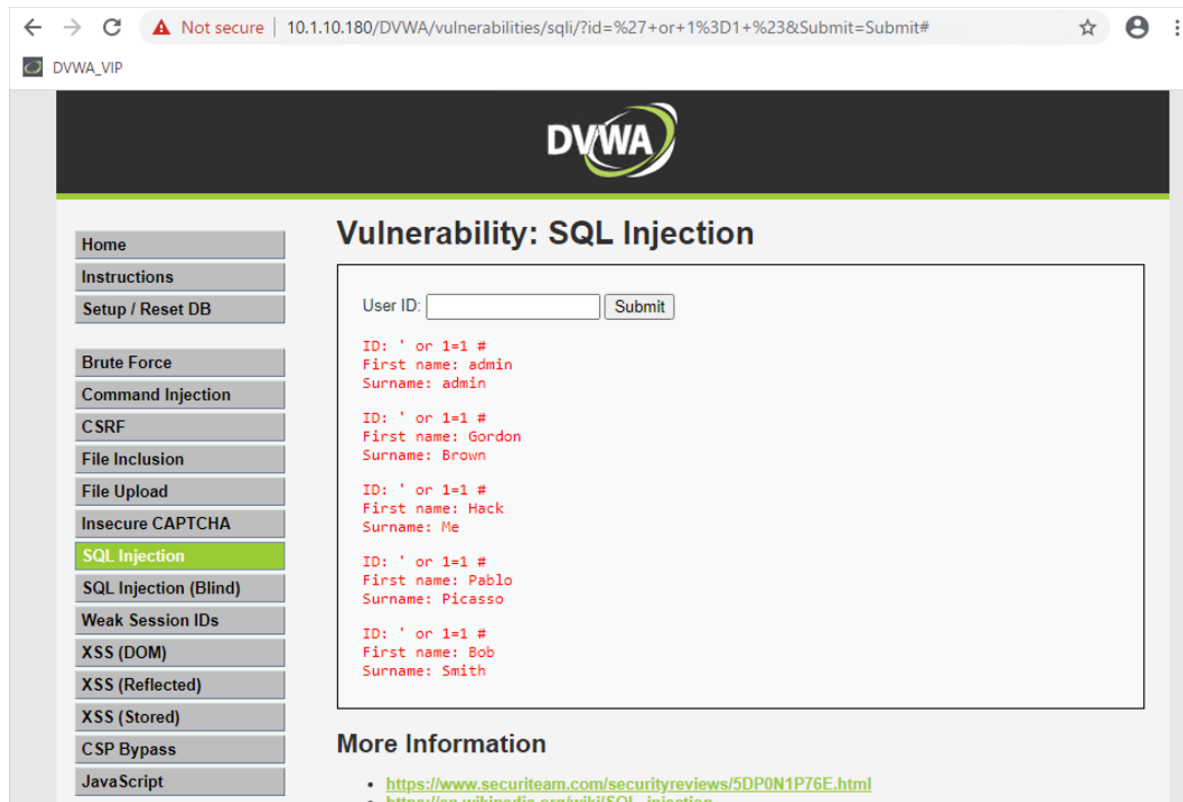


4. 作成済みの Logging Profile(s) をアタッチします。

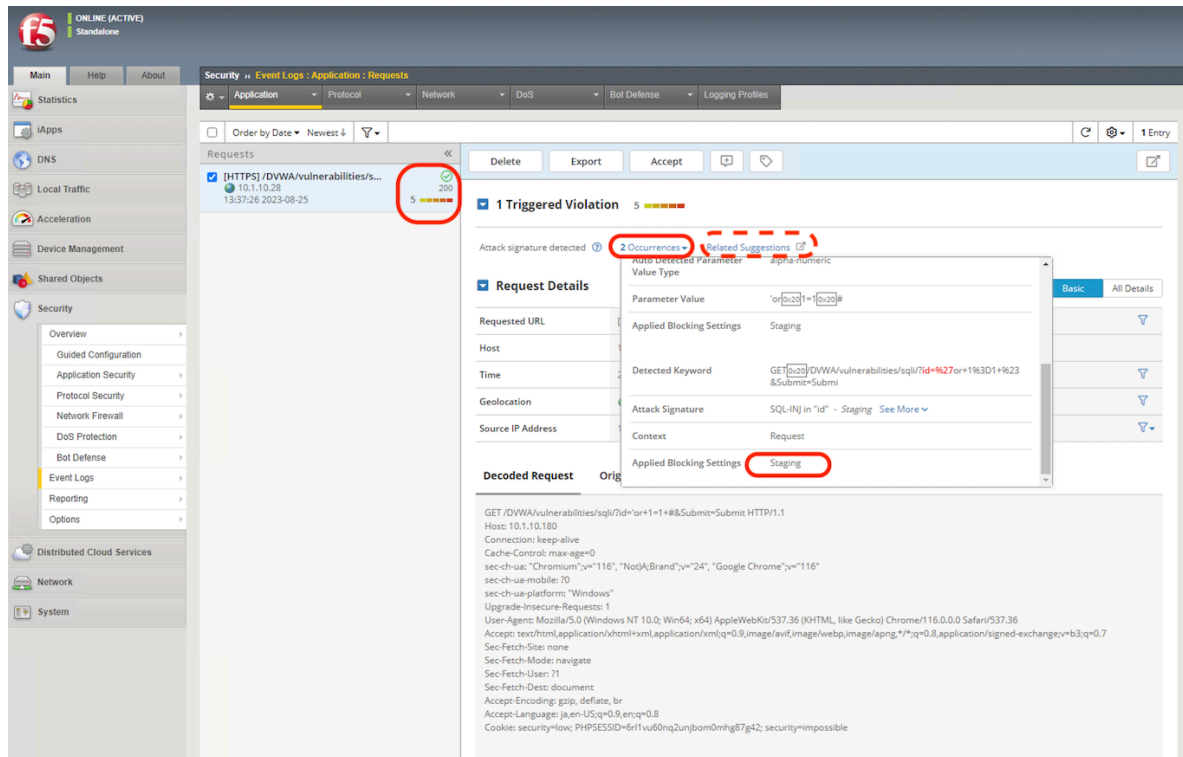


2.1.8 シグネチャの動作確認

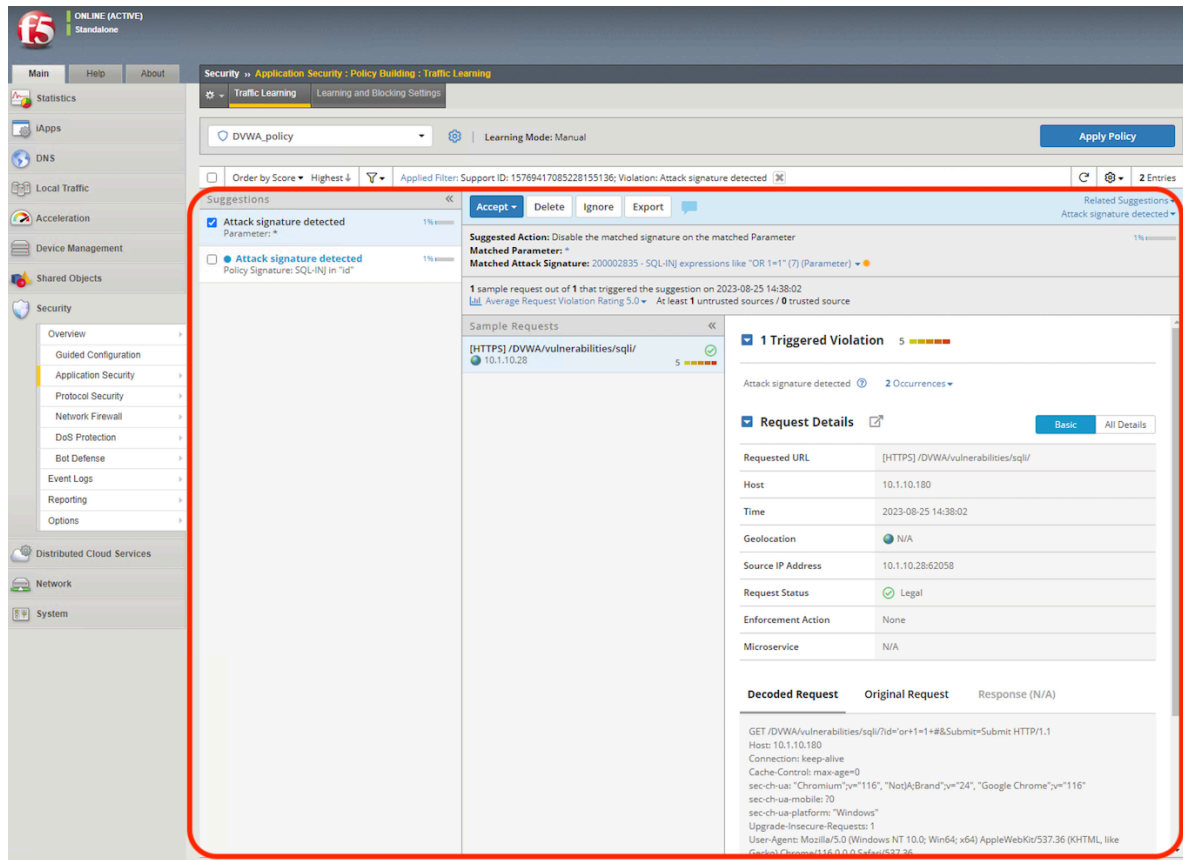
1. Windows クライアントを起動し、<https://10.1.10.180/DVWA/login.php> にアクセスします。Username: **admin**、Password: **password** でログインし、**SQL Injection** にアクセスし、User ID に '**or 1=1 #** と入力し、SQL インジェクション攻撃をします。(本ガイドからコマンドはコピーしないで下さい。シングルクォーテーションに注意してタイプして下さい。)



2. Security >> Event Logs : Application : Requests にて、Staged で SQL インジェクションが検出されていることを確認します。



3. 上記画面の Suggestions の **Related Suggestions** をクリックすると、TrafficLearning の画面でも **Attack signature detected** が確認できます。(Security >> Application Security : Policy Building : Traffic Learning でもたどれます。)



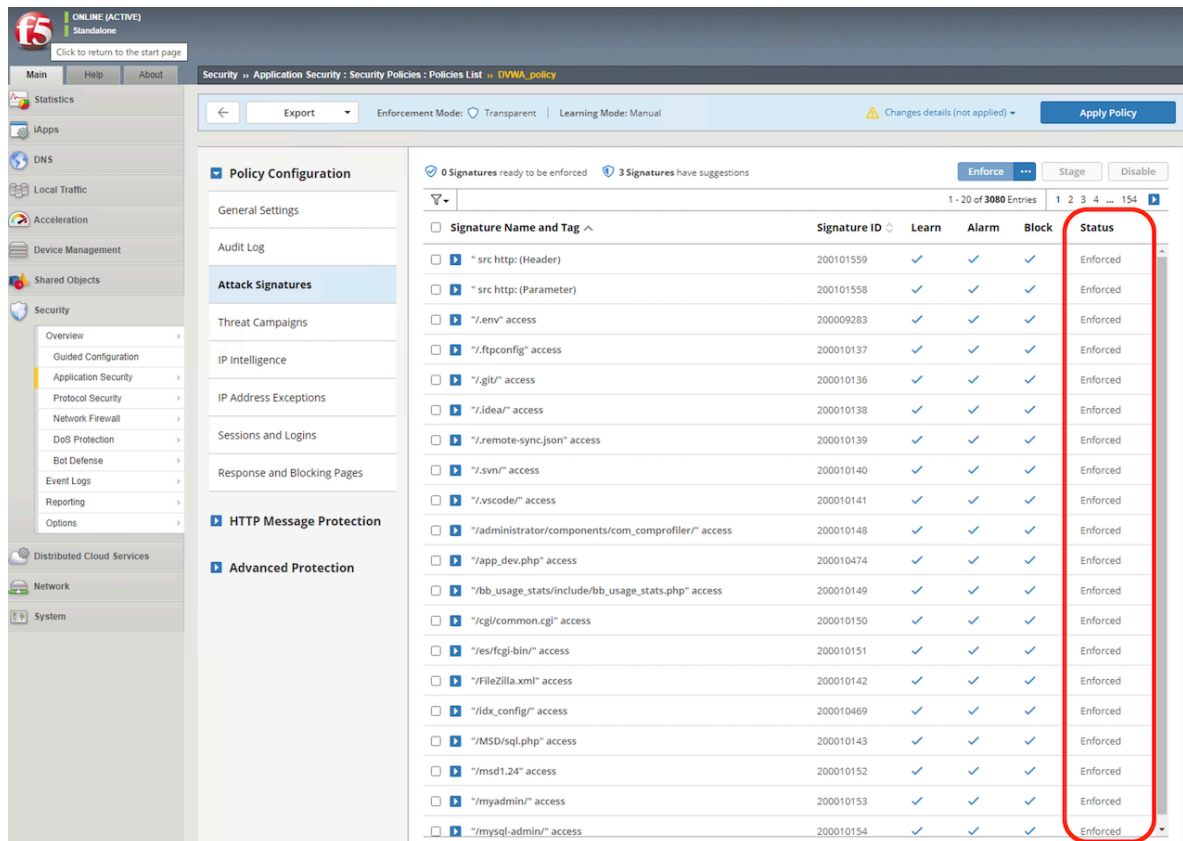
2.1.9 シグネチャのステージング解除

1. ステージングを解除すると、Event log に攻撃として記録されます。Security >> Application Security : Security Policies : Policies List >> DVWA_policy にて、Attack Signatures を選択し、画面右上の Enforce all Staged Signatures を選択し、ステージングを解除します。

The screenshot shows the 'Policy Configuration' page for 'OVWA_policy'. The 'Attack Signatures' section is active, displaying a list of 15 signatures. The 'Status' column for all signatures is 'Staging'. A red box highlights the 'Enforce' button and the 'Status' column.

Signature Name and Tag	Signature ID	Learn	Alarm	Block	Status
<input type="checkbox"/> "src http: (Header)"	2000101559	✓	✓	✓	Staging
<input type="checkbox"/> "src http: (Parameter)"	2000101558	✓	✓	✓	Staging
<input type="checkbox"/> "/.env/" access	200009283	✓	✓	✓	Staging
<input type="checkbox"/> "/ftpconfig/" access	200010137	✓	✓	✓	Staging
<input type="checkbox"/> "/.git/" access	200010136	✓	✓	✓	Staging
<input type="checkbox"/> "/.idea/" access	200010138	✓	✓	✓	Staging
<input type="checkbox"/> "/remote-sync.json" access	200010139	✓	✓	✓	Staging
<input type="checkbox"/> "/.svn/" access	200010140	✓	✓	✓	Staging
<input type="checkbox"/> "/.vscode/" access	200010141	✓	✓	✓	Staging
<input type="checkbox"/> "/administrator/components/com_comprofiler/" access	200010148	✓	✓	✓	Staging
<input type="checkbox"/> "/app_dev.php" access	200010474	✓	✓	✓	Staging
<input type="checkbox"/> "/bb_usage_stats/include/bb_usage_stats.php" access	200010149	✓	✓	✓	Staging
<input type="checkbox"/> "/cgi/common.cgi" access	200010150	✓	✓	✓	Staging
<input type="checkbox"/> "/es/cgi-bin/" access	200010151	✓	✓	✓	Staging
<input type="checkbox"/> "/FileZilla.xml" access	200010142	✓	✓	✓	Staging
<input type="checkbox"/> "/idx_config/" access	200010469	✓	✓	✓	Staging
<input type="checkbox"/> "/MSD/sql.php" access	200010143	✓	✓	✓	Staging
<input type="checkbox"/> "/msd1.24" access	200010152	✓	✓	✓	Staging
<input type="checkbox"/> "/myadmin/" access	200010153	✓	✓	✓	Staging
<input type="checkbox"/> "/mysql-admin/" access	200010154	✓	✓	✓	Staging

2. ステージングが解除されると、Status が Enforced となります。



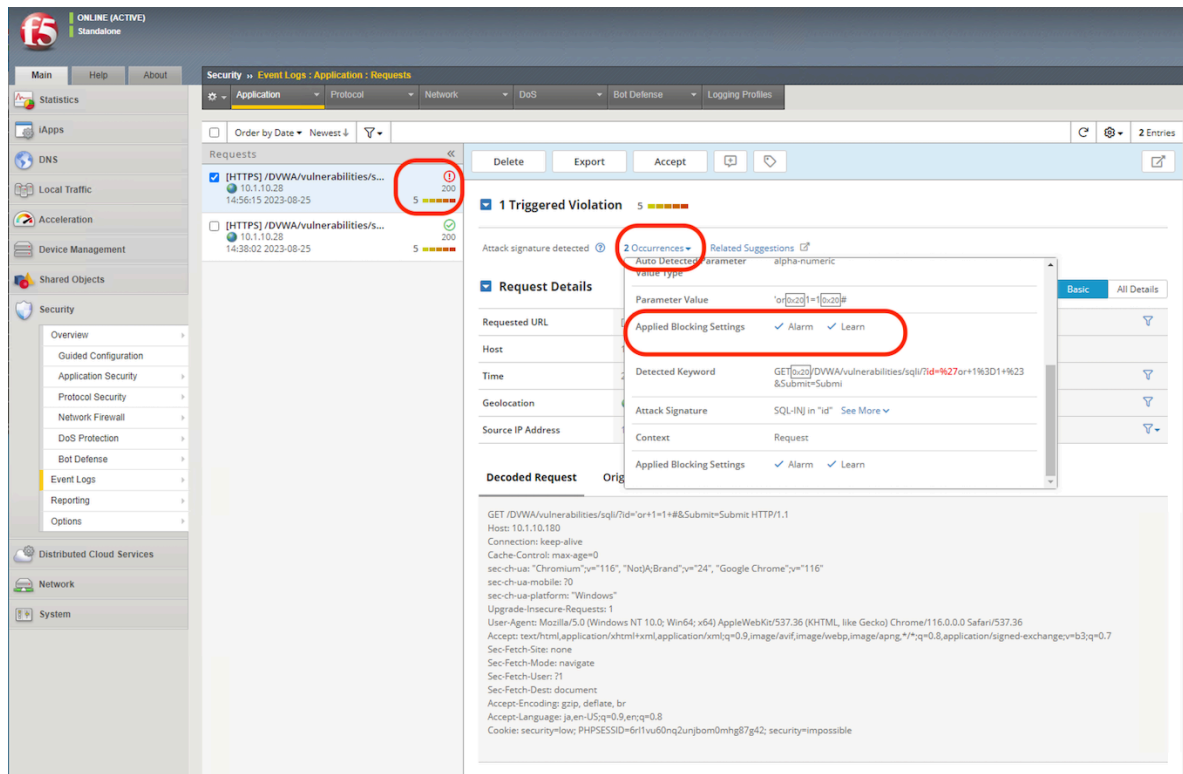
3. Apply Policy を押します。



4. 再度 Windows クライアントから SQL インジェクションを試みます。

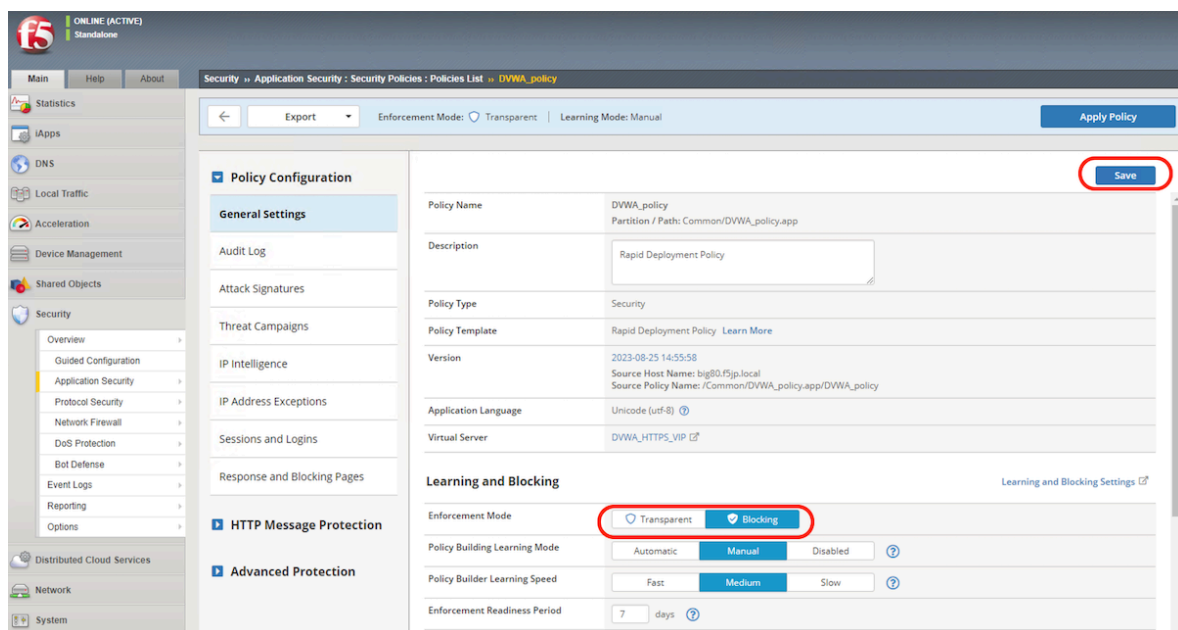


5. **Security >> Event Logs : Application : Requests** にて、**Alarm Learn** で SQL インジェクションが検出されていることを確認します。

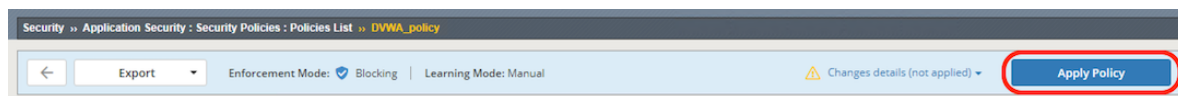


2.1.10 Blocking モードへの変更

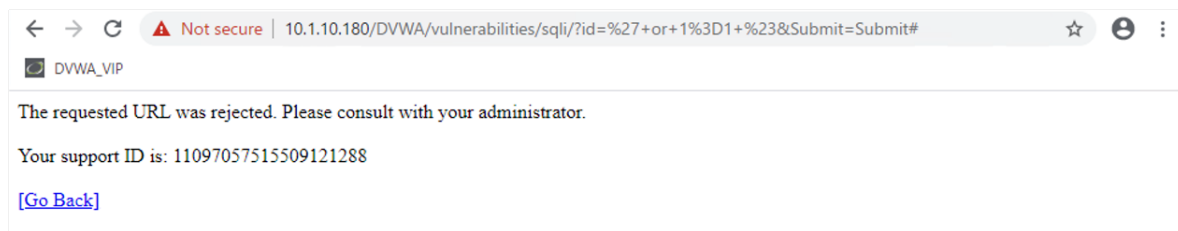
1. Blocking モードへ変更すると、Event log に攻撃として記録され、更にブロックされます。**Security >> Application Security : Security Policies : Policies List >> DWA_policy** にて、**General Settings** を選択し、**Enforcement Mode** を **Blocking** に変更し、**Save** ボタンを選択します。



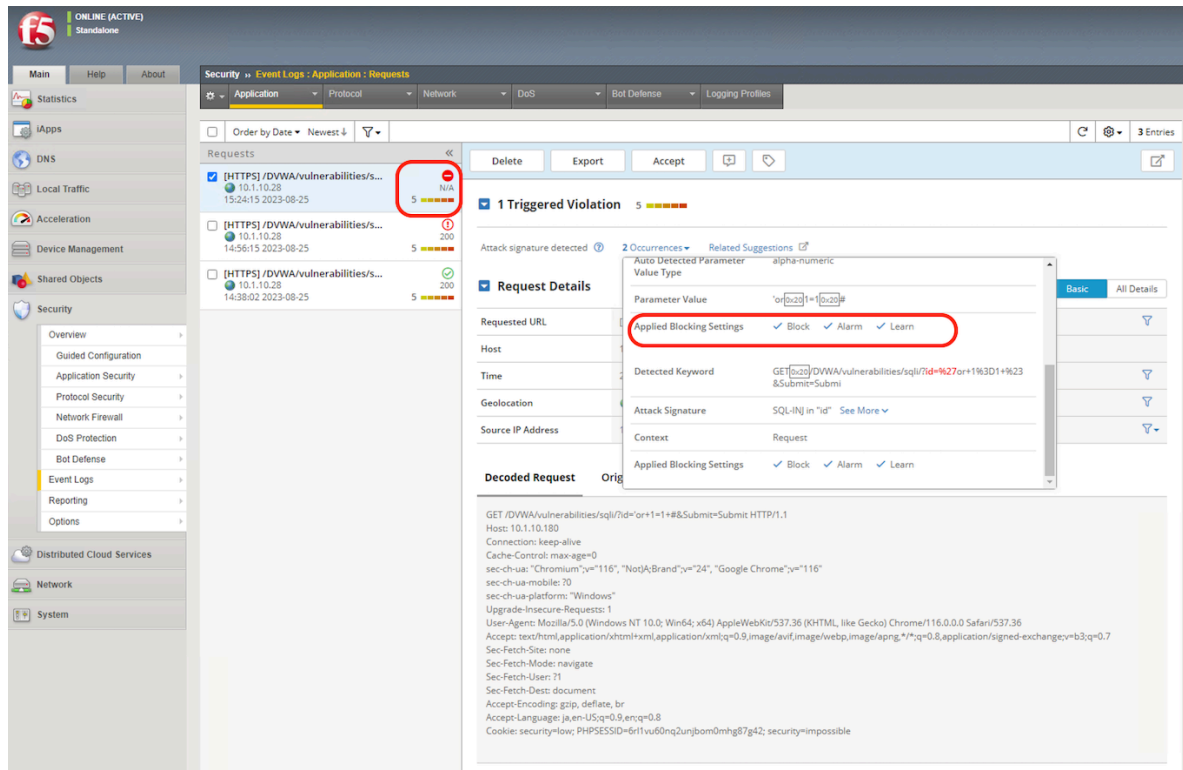
2. Apply Policy を押します。



3. 再度 Windows クライアントから SQL インジェクションを試みます。



4. Security >> Event Logs : Application : Requests にて、Block Alarm Learn で SQL インジェクションが検出されていることを確認します。

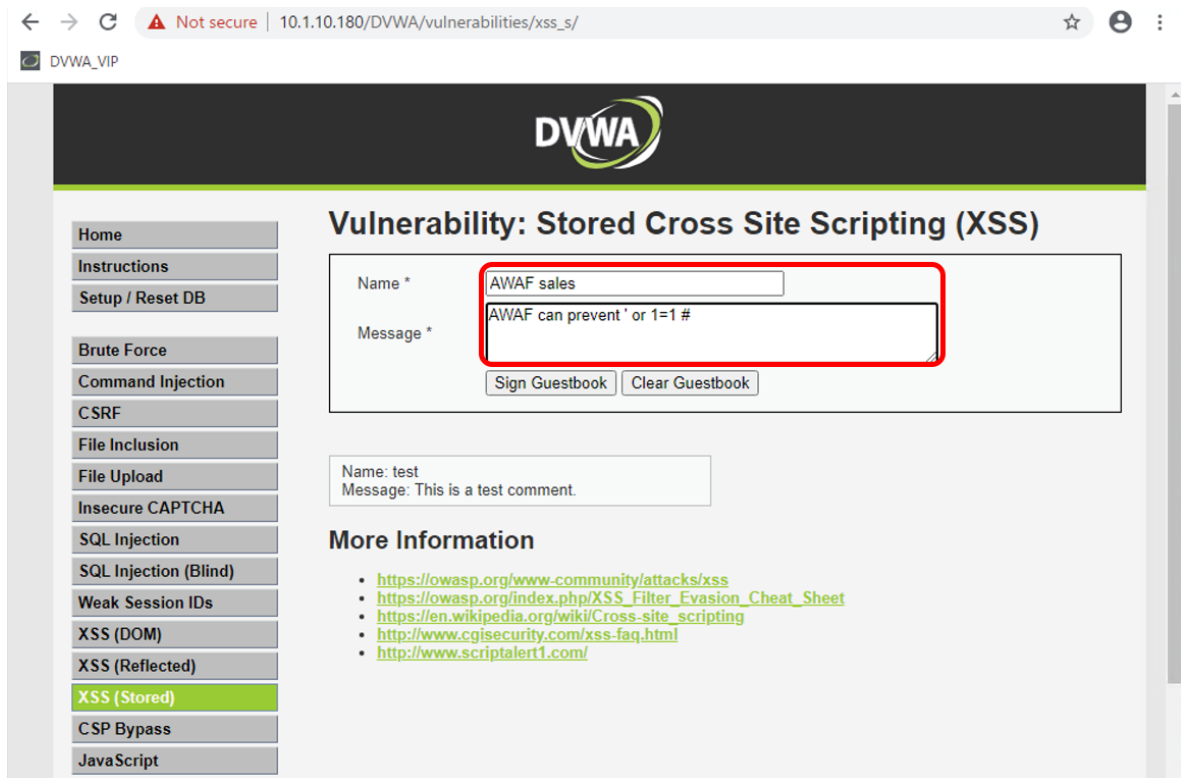


2.1.11 シグネチャのチューニング

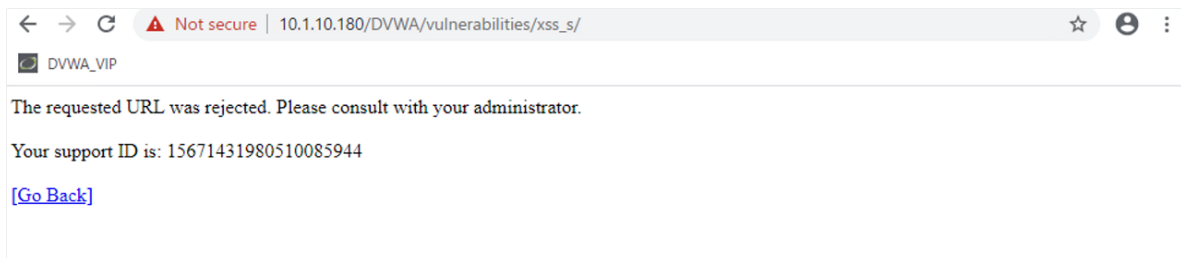
誤検知が発生した場合の対処例をご紹介します。以下で実施する内容は、Web アプリケーションの各パラメータの役割が全て把握できている場合を除き、運用開始前から全てを設定するのは難しいかもしれません。その場合は、仮運用・本運用に入ってから、再度このチューニングを実施してください。

以下は誤検知の例です。

1. 入力内容にたまたま攻撃に関連するパラメータが含まれてしまったとします。



2. 書き込みを行うと、AWAF で攻撃として検知されてしまいます。



以降、2つの対策例をご紹介します。

誤検知したパラメータをホワイトリスト化

1. Event log で誤検知したログを確認します。

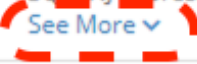
The screenshot displays the AWAF v17.1 web interface. On the left, the 'Security' menu is expanded, showing 'Event Logs' as the selected option. The main panel is titled 'Security > Event Logs : Application : Requests'. It shows a list of requests with columns for 'Requests', 'Status', and 'Score'. One request is highlighted with a red box, showing a 'Triggered Violation' for the URL '[HTTPS] /DWA/vulnerabilities/xss_s/'. The right panel shows the details of this violation, including the 'Request Details' table and the 'Decoded Request' section.

Requested URL	[HTTPS] /DWA/vulnerabilities/xss_s/	Request Status	Blocked
Host	10.1.10.180	Enforcement Action	Block
Time	2023-08-25 15:31:08	Virtual Server	DWA_HTTPS_VIP
Geolocation	N/A	Security Policy	DWA_policy
Source IP Address	10.1.10.28:64910	Microservice	N/A

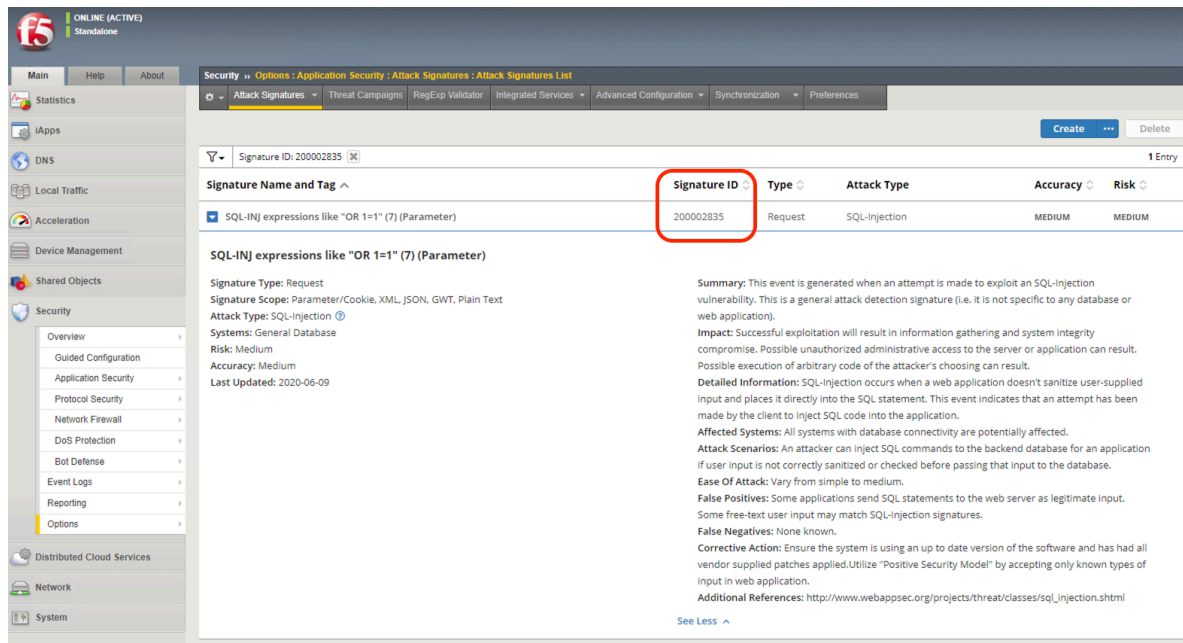
Decoded Request

```
POST /DWA/vulnerabilities/xss_s/ HTTP/1.1
Host: 10.1.10.180
Connection: keep-alive
Content-Length: 86
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="116", "Not(A.Brand);v="24", "Google Chrome";v="116"
sec-ch-ua-mobile: 70
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://10.1.10.180
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://10.1.10.180/DWA/vulnerabilities/xss_s/
Accept-Encoding: gzip, deflate, br
Accept-Language: ja,en-US;q=0.9,en;q=0.8
Cookie: security=low; PHPSESSID=6r11vu0nq2unjbom0mhg87g42; security=impossible
txtName=AWAF+sales&mtbMessage=AWAF+can+prevent+*or+1+1+1#&btnSign=Sign+Guestbook
```

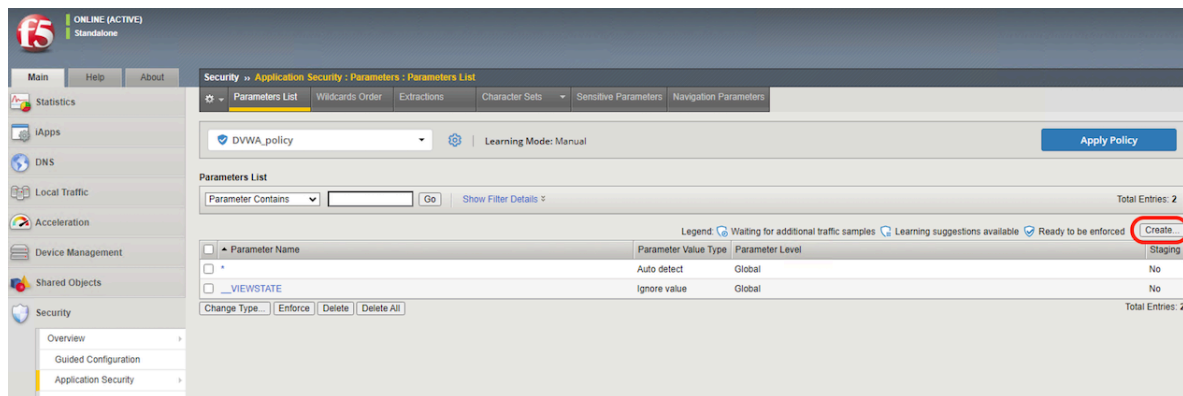
2. **Occurrences** をクリックし、誤検知したパラメータ名 (mtbMessage) を確認します。また、Attack Signature 列の See More をクリックし、Documentation リンクを開いたページで、シグネチャ ID (200002835) を確認します。

Detected Keyword	mtxMessage=AWAF0x20can0x20prevent0x20or0x201=10x20#
Attack Signature	SQL-INJ expressions like "OR 1=1" (7) (Parameter) See More 
Context	Parameter (detected in Form Data)
Parameter Level	Global
Actual Parameter Name	mtxMessage
Wildcard Parameter Name	*
Auto Detected Parameter Value Type	alpha-numeric

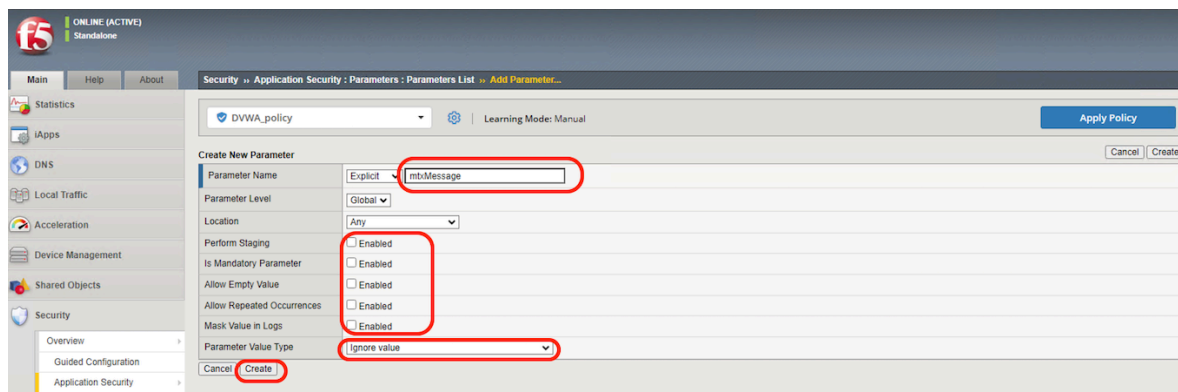
Medium
User-defined
No
Revision
4
Last Updated
06/09/2020
Documentation
Documentation
Context
Parameter (detected in Form Data)
Parameter Level
Global
Actual Parameter Name
mtxMessage
Wildcard Parameter Name
*



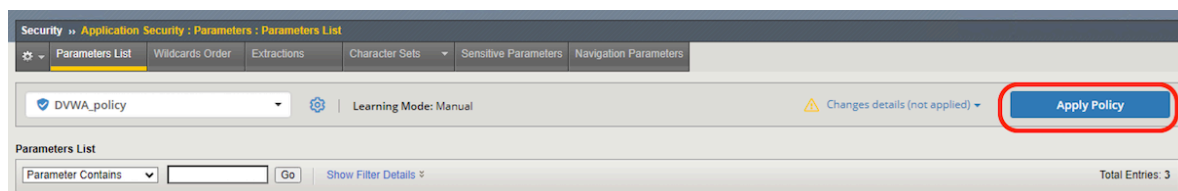
3. Security >> Application Security : Parameters : Parameters List にて、Create ボタンを押します。



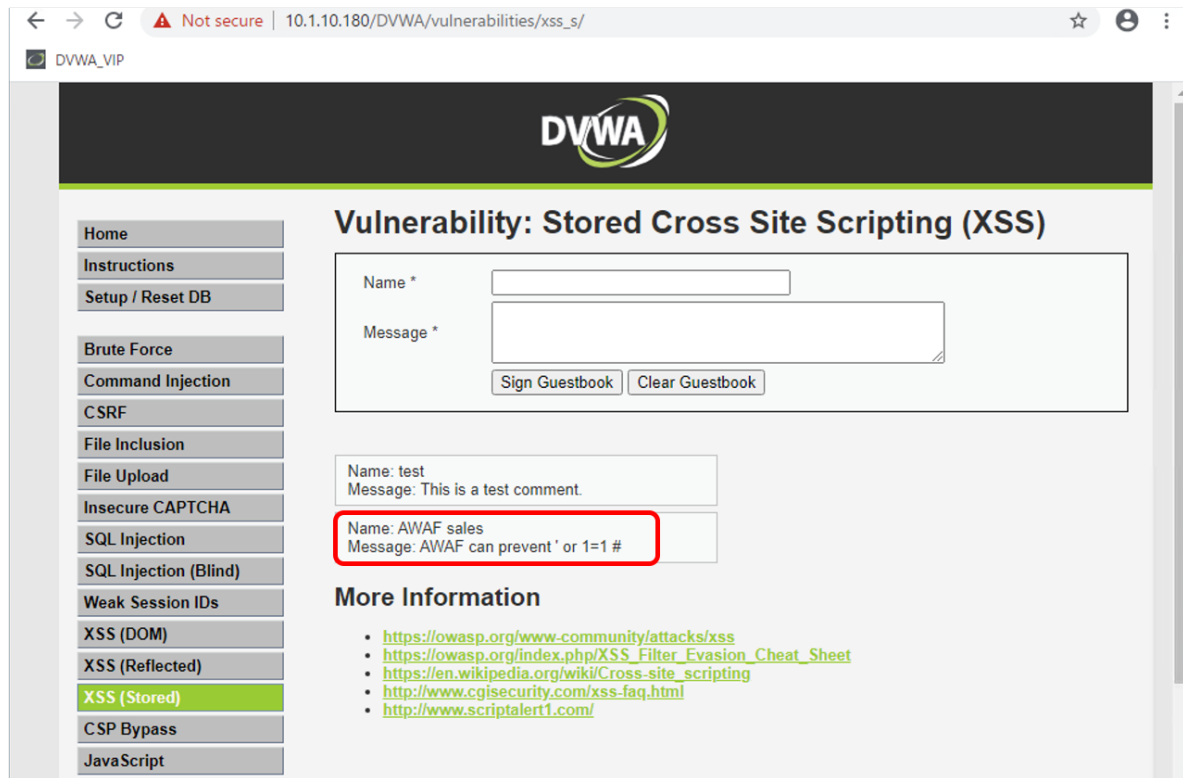
4. Parameter Name に誤検知したパラメータ名 (mtxMessage) を入力し、チェック BOX をすべてクリアし、Parameter Value Type にて、Ignore Value を選択し、Create ボタンを押します。



5. *Apply Policy* を押します。

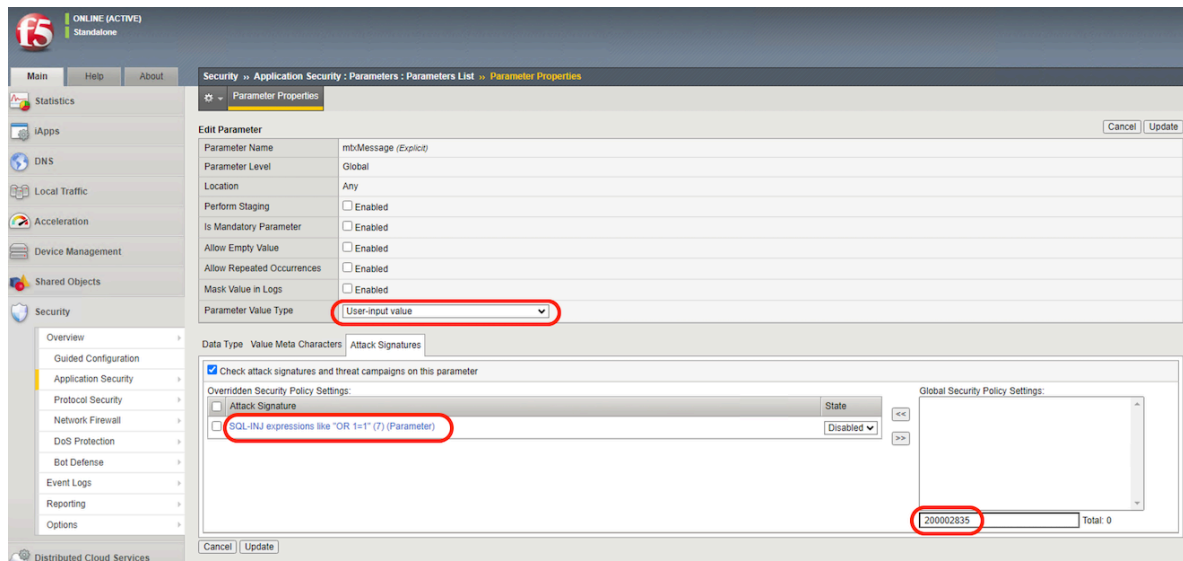


6. Windows にて再度書き込みを行うと、書き込みが成功することを確認します。

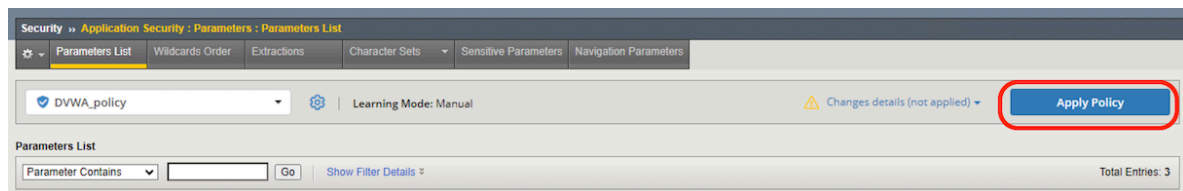


誤検知したパラメータで該当シグネチャを無効化

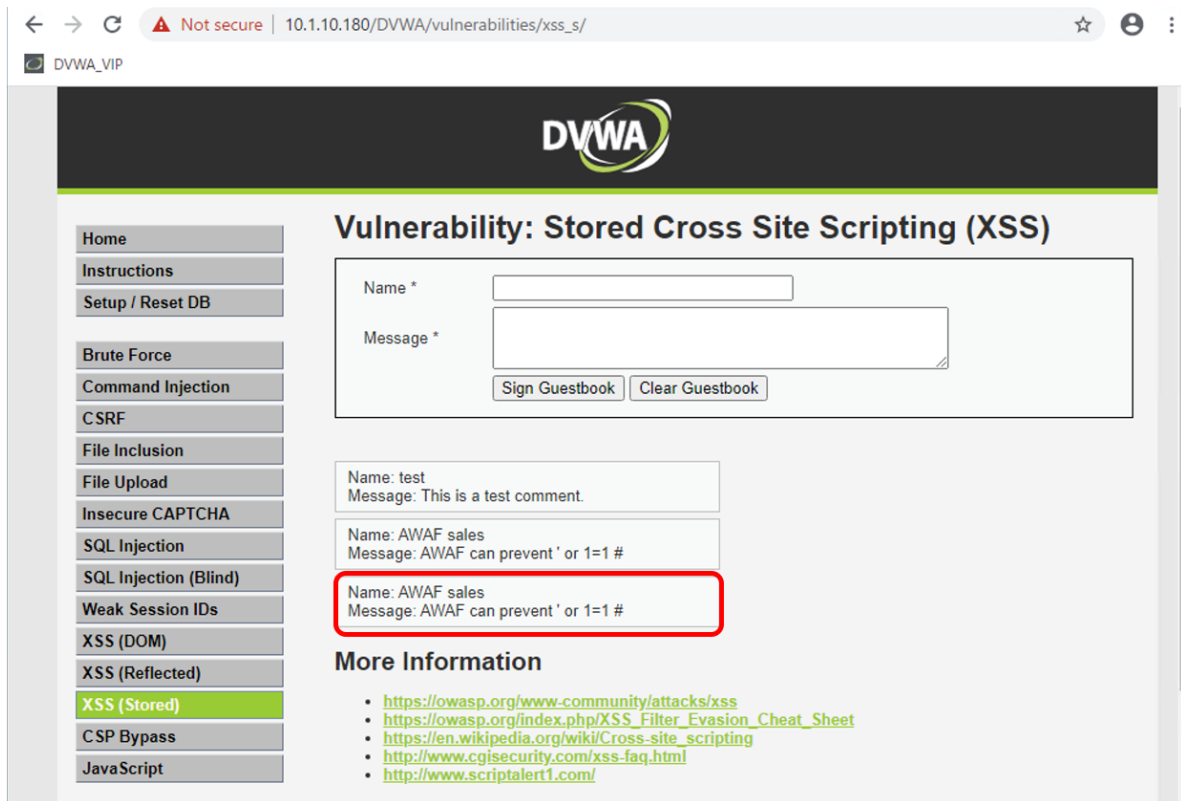
1. 今度は先程作成した Parameter の **Parameter Value Type** にて、**User-Input Value** を選択し、**Attack Signatures** タブにて、誤検知したシグネチャ ID (200002835) を左に移動し、**Disabled** にし、**Update** ボタンを押します。



2. Apply Policy を押します。



3. Windows にて再度書き込みを行うと、書き込みが成功することを確認します。



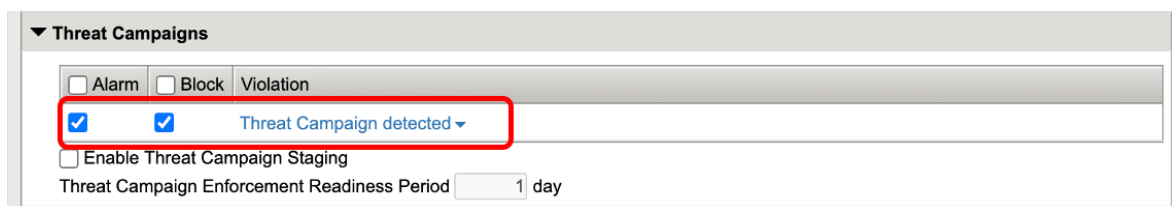
2.1.12 Threat campaigns シグネチャの設定

Web アプリケーションの脅威対策を行う上で、実際の攻撃とフォールスポジティブを見極めることに直面することがあります。シグネチャや WAF の様々な機能によって、既知の脆弱性に対する攻撃リクエストを評価すると同時に、悪意のないリクエストも評価されるため、管理者は WAF で検知されたアラートに対し、正常なリクエストか悪意のあるリクエストか判断を迫られることがあります。

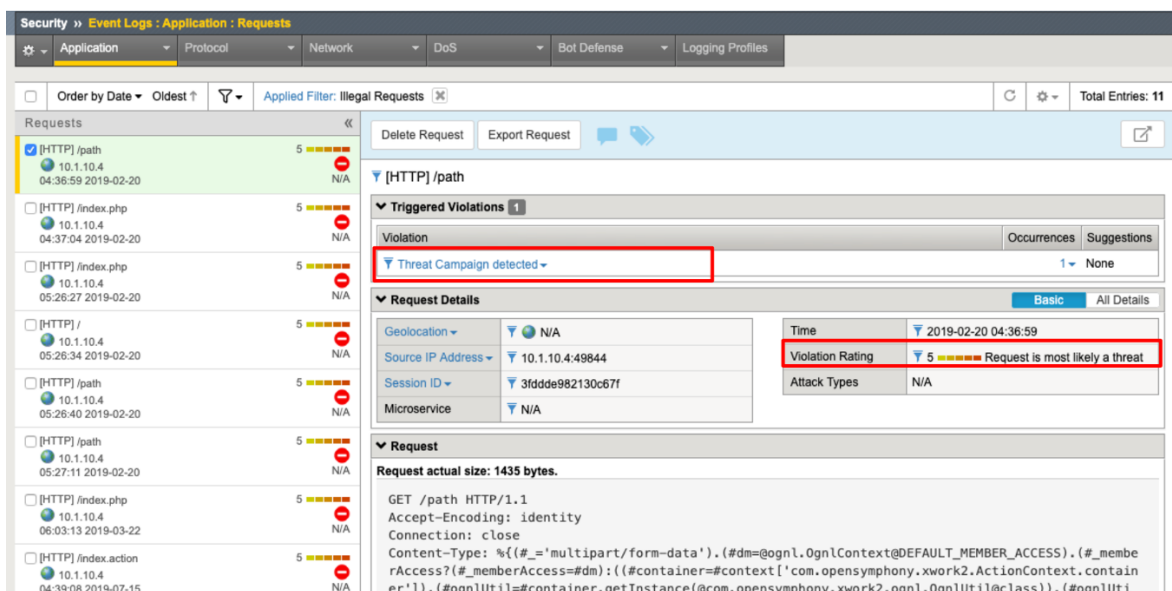
この問題は、検査するデータがシングルポイントであることにあります。もっと多くの条件を元にリクエストを検査することによって、この問題を解決することができるとあります。F5 はこの問題を解決する手法として、**Threat Campaigns** シグネチャ という独自のシグネチャを提供しています。**Threat Campaigns** シグネチャは、実際の攻撃キャンペーンを元に複数の条件をマッピングされたものになっています。

この項では、Threat Campaigns シグネチャの設定確認と、テキスト上にて攻撃サンプルログを確認します。

1. **Security >> Application Security : Policy Building : Learning and Blocking Settings** で表示された画面にて、Threat Campaigns の **Alarm** と **Block** が有効になっていることを確認します。(Learn は存在しません。)



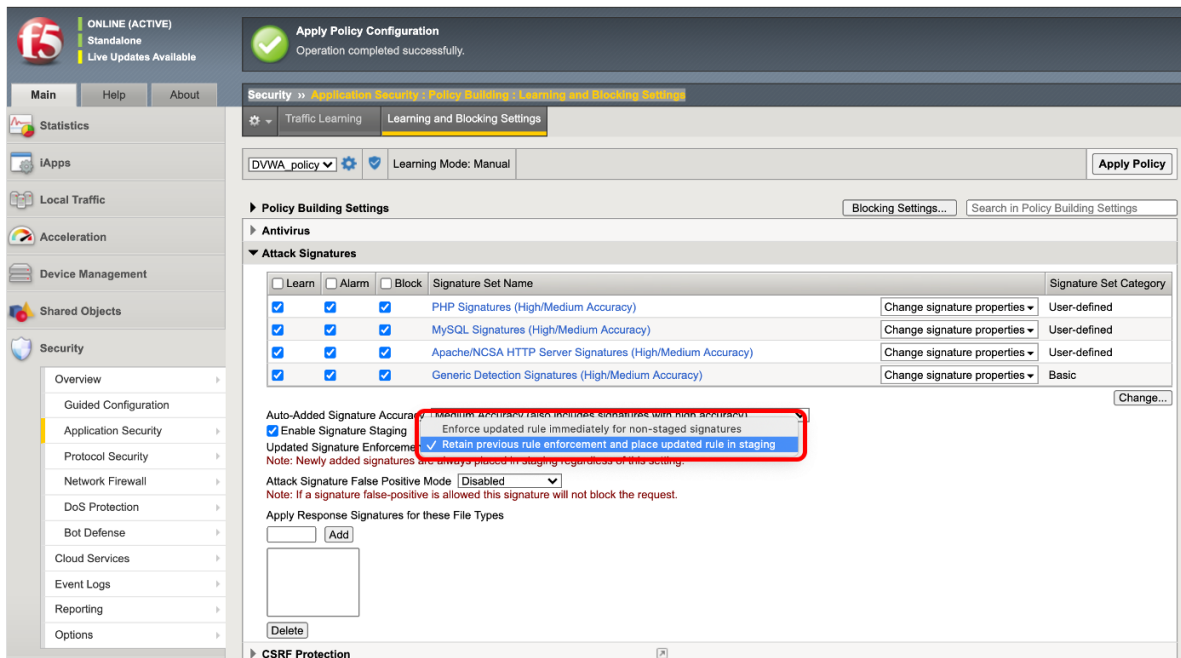
2. 攻撃を受けたと仮定して、Eveng Logs でログを確認します。(F5 ハンズオンでは実際に攻撃は行いません。本ガイドによる確認のみとなります。) 下記は攻撃を受けたときのサンプルログとなります。こちらを見ると、Violation Rating が **5:Request is most likely a threat** となっていることが分かります。これは Threat Campaigns シグネチャが実際の攻撃を元に作成されており、ほぼフォールスポジティブではないことを表しています。



注釈: Threat Campaigns シグネチャを利用するには、別途サブスクリプションライセンスが必要となります。

2.1.13 シグネチャ、TC シグネチャのアップデート

- シグネチャが更新された場合に、ステージングモードで運用するか、即座に Learn/Alarm/Block の設定を適用するかの指定が可能です。また、既存シグネチャの更新後の振る舞いについての指定も可能です。
Security >> Application Security : Policy Building : Learning and Blocking Settings の Attack Signaturesにて表示された画面で、必要に応じて希望する動作への設定変更を実施します。(変更する場合、Save, ApplyPolicy で反映させます。)



注釈:

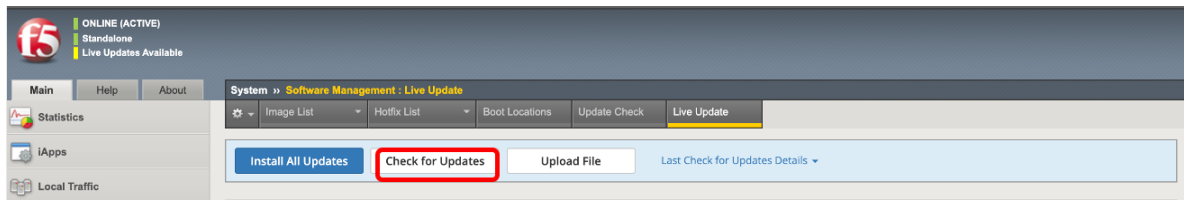
Enforce updated rule immediately for non-staged signatures:

Enforcement 状態 (Non-Staging) の既存シグネチャがアップデートされた場合、更新されたシグネチャも Non-Staging とします。

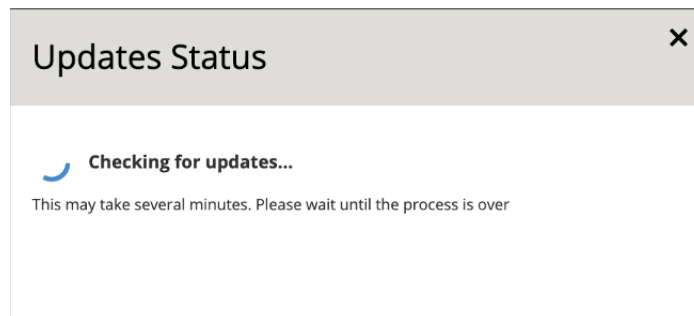
Retain previous rule enforcement and place updated rule in staging:

Enforcement 状態 (Non-Staging) の既存シグネチャがアップデートされた場合、更新前のシグネチャは Non-Staging のままとし、更新されたシグネチャを Staging とします。更新されたシグネチャの Staging 期間が終了した際に、更新前のシグネチャが削除され、更新されたシグネチャが Non-Staging となります。(Manual モードでの運用の場合は、手動で Staging->Non-Staging の設定が必要です。)

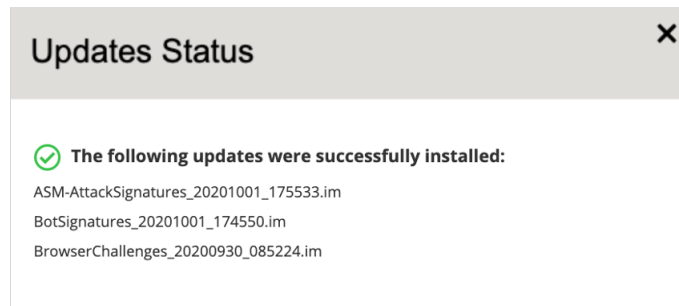
2. **System >> Software Management : Live Update** で表示された画面で、**Check for Updates** をクリックして、シグネチャ更新の有無を確認します。



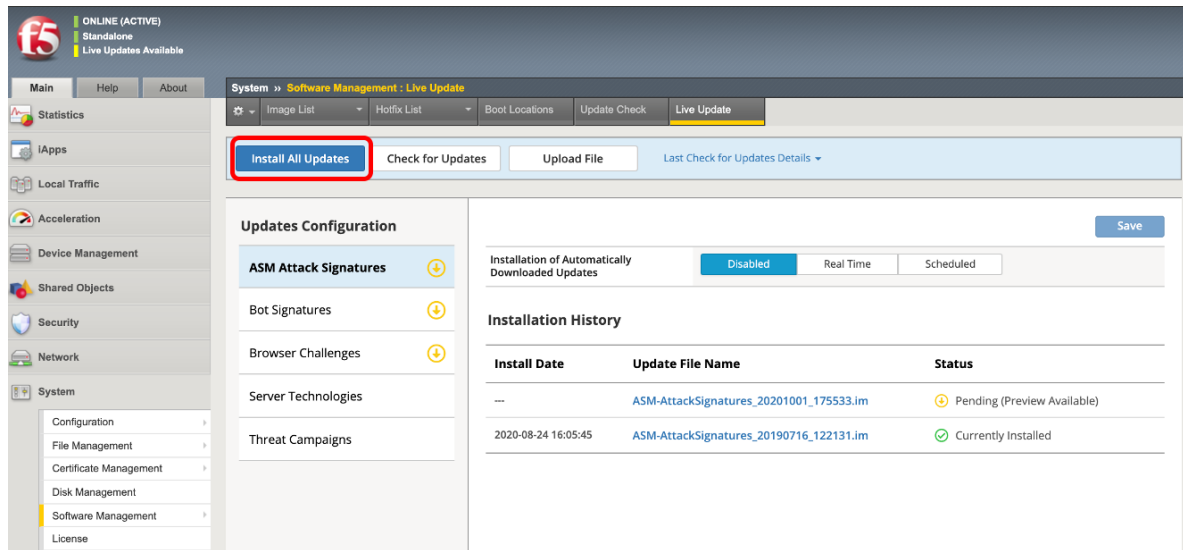
3. チェック中のイメージです。(チェックには数分かかります。)



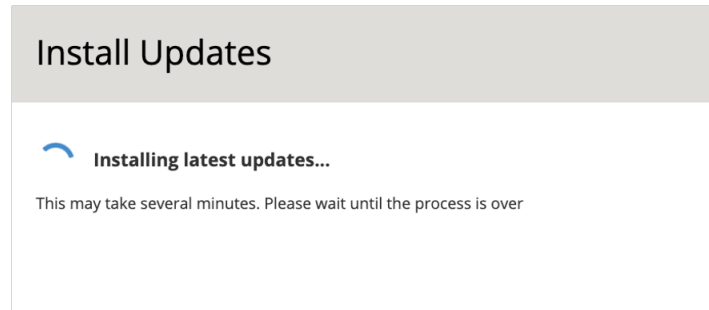
4. 更新可能なシグネチャがある場合、以下のように表示されます。を押し、画面を閉じます。(既にシグネチャを裏でダウンロード済みの場合は、**No updates found** と表示されます。ダウンロード済みのシグネチャは黄色い矢印アイコンが表示され、**Pending Status** となっています。)



5. 全てをインストールしたい場合は、InstallAllUpdates をクリックします。



6. シグネチャ更新中は、以下のように表示されます。(更新には数分かかります。)



7. Install が完了すると以下ようになります。を推し、画面を閉じます。

Install Updates



✓ The following updates were successfully installed:

ASM-AttackSignatures_20201001_175533.im

BotSignatures_20201001_174550.im

BrowserChallenges_20200930_085224.im

8. 以下が更新後のイメージとなります。CurrentlyInstalled ステータスのシグネチャをクリックします。

System » Software Management : Live Update

Image List | Hotfix List | Boot Locations | Update Check | **Live Update**

Install All Updates | Check for Updates | Upload File | Last Check for Updates Details ▾

Updates Configuration

ASM Attack Signatures

Bot Signatures

Browser Challenges

Server Technologies

Threat Campaigns


Installation of Automatically Downloaded Updates: **Disabled** | Real Time | Scheduled

Installation History

Install Date	Update File Name	Status
2020-10-04 21:05:05	ASM-AttackSignatures_20201001_175533.im	✓ Currently Installed
2020-08-24 16:05:45	ASM-AttackSignatures_20190716_122131.im	Previously Installed


9. Update された Signature の情報が表示されます。各 Entity をクリックすると、該当するシグネチャー一覧が確認できます。


Installation Details

Update File Name	ASM-AttackSignatures_20201001_175533.im
Create Date	2020-10-02 02:55:33
Install Date	2020-10-04 21:05:05
Readme	Added Cross Site Scripting (XSS) signature 200101588 for import() (Parameter) Added Cross Site Scripting (XSS) signature 200101589 for import() (H... View Full Readme
Status	 Currently Installed

Install Results

Deleted Entities (0)

 Added Entities (1513)

 Modified Entities (1653)

InstallDeleteCancel

10. Update がない場合は Install Updates をクリックしても以下のように表示されます。

Updates Status

No updates found

11. 追加されたシグネチャがステージングになっているかどうかの確認方法を示します。Security >> Application Security : Security Policies : Policies List >> DVWA_policy で表示された画面で、Status を Staging でフィルタリングします。

Security » Application Security : Security Policies : Policies List » DVWA_policy

← Export ▾

Security Policy Configuration

- General Settings
- Inheritance Settings
- Microservices
- Attack Signatures**
- Threat Campaigns
- Response and Blocking Pages

0 Signatures ready to be enforced 2 Signatures have suggestions

▽

Basic

Advanced

Attack Signature Name

Status

Signature ID

User-Defined

Signature Scope

Signature Type

Attack Type

Systems

12. 追加されたシグネチャがステージングとなっていることが分かります。

Security » Application Security : Security Policies : Policies List » DVWA_policy

← Export ▾ Apply Policy

Security Policy Configuration

- General Settings
- Inheritance Settings
- Microservices
- Attack Signatures**
- Threat Campaigns
- Response and Blocking Pages

0 Signatures ready to be enforced 2 Signatures have suggestions Enforce ... Stage Disable

▼ Status: Staging ✕ 1 - 20 of 885 Entries 1 2 ... 45 ▾

<input type="checkbox"/> Signature Name ^	Signature ID	Learn	Alarm	Block	Status
<input type="checkbox"/> ▶ "system" injection attempt (Header)	200004200	✓	✓	✓	Staging
<input type="checkbox"/> ▶ "system" injection attempt (Parameter)	200004199	✓	✓	✓	Staging
<input type="checkbox"/> ▶ "system" injection attempt (URI)	200004201	✓	✓	✓	Staging
<input type="checkbox"/> ▶ "vBulletin widgetConfig Render Code E...	200004995	✓	✓	✓	Staging
<input type="checkbox"/> ▶ <script>alert(1);</script> (Header)	200101610	✓	✓	✓	Staging
<input type="checkbox"/> ▶ <script>alert(1);</script> (Parameter)	200101609	✓	✓	✓	Staging
<input type="checkbox"/> ▶ alert() (3) (Header)	200101624	✓	✓	✓	Staging
<input type="checkbox"/> ▶ alert() (3) (Parameter)	200101623	✓	✓	✓	Staging
<input type="checkbox"/> ▶ alert() (3) (URI)	200101625	✓	✓	✓	Staging
<input type="checkbox"/> ▶ AngularJS Sandbox Escape - constructo...	200101352	✓	✓	✓	Staging
<input type="checkbox"/> ▶ AngularJS Sandbox Escape - constructo...	200101351	✓	✓	✓	Staging
<input type="checkbox"/> ▶ AngularJS Sandbox Escape - constructo...	200101353	✓	✓	✓	Staging
<input type="checkbox"/> ▶ Apache mod_proxy Connection DoS	200012065	✓	✓	✓	Staging
<input type="checkbox"/> ▶ autofocus (Header)	200001582	✓	✓	✓	Staging
<input type="checkbox"/> ▶ autofocus (Parameter)	200001581	✓	✓	✓	Staging
<input type="checkbox"/> ▶ autofocus (URI)	200001718	✓	✓	✓	Staging
<input type="checkbox"/> ▶ CodeIgniter RCE Gadget Chain	200104348	✓	✓	✓	Staging

注釈: F5 ハンズオンでは手順の関係上、動作確認の後にシグネチャをアップデートしておりますが、本来は運用テスト前に行ってください。新しいシグネチャをアップデートすることで新たな攻撃に対応することができます。シグネチャの更新についての詳細は、以下の記事を参考にして下さい。

- [K82512024: Managing BIG-IP ASM Live Updates \(14.1.x and later\)](#)

2.1.14 CVE 番号によるシグネチャの検索

各シグネチャがどの CVE に対応しているか確認することが可能です。

1. **Security >> Options : Application Security : Attack Signatures : Attack Signature List** で表示された画面のフィルタマークをクリックすると、以下のような画面が表示されます。 **ADVANCED** タブを選択し、**References** から **CVE** を選択し、CVE 番号を入力して **Apply** ボタンを押すと、該当するシグネチャが表示されます。

The first screenshot shows the 'Attack Signatures' list with the 'ADVANCED' tab selected. The 'References' dropdown is set to 'CVE', and the CVE number '2017-5638' is entered. The 'Apply' button is highlighted.

The second screenshot shows the filtered results for CVE 2017-5638. The search criteria are 'CVE reference contains: 2017-5638'. The results are displayed in a table with columns: Signature Name and Tag, Signature ID, Type, Attack Type, Accuracy, and Risk.

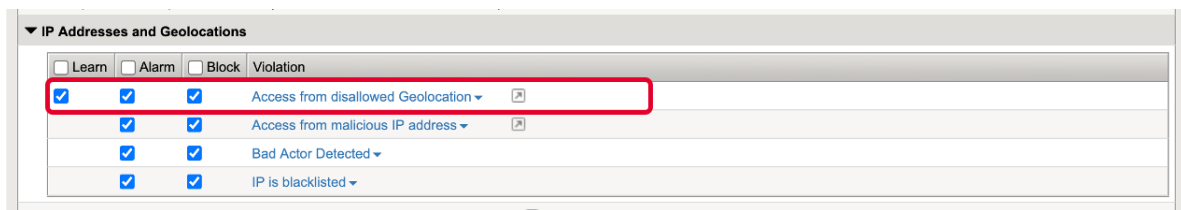
Signature Name and Tag	Signature ID	Type	Attack Type	Accuracy	Risk
Code Injection Java (Accessing attributes)	200004156	Request	Server Side Code Injection	MEDIUM	MEDIUM
Code Injection Java (Accessing attributes) (#_classResolver)	200004262	Request	Server Side Code Injection	LOW	HIGH
Code Injection Java (Accessing attributes) (#_keepLastEvaluation)	200004265	Request	Server Side Code Injection	LOW	HIGH
Code Injection Java (Accessing attributes) (#_lastEvaluation)	200004264	Request	Server Side Code Injection	LOW	HIGH
Code Injection Java (Accessing attributes) (#_traceEvaluations)	200004263	Request	Server Side Code Injection	LOW	HIGH
Code Injection Java (Accessing attributes) (#_typeResolver)	200004261	Request	Server Side Code Injection	LOW	HIGH
Java code injection - Content-Type class github.com/joamatosfr/jexboss	200004287	Request	Server Side Code Injection	HIGH	HIGH
Java code injection - Content-Type class org.jboss.console.remote.RemoteMBeanInvocation	200004286	Request	Server Side Code Injection	HIGH	HIGH
Java code injection - jexboss webshell	200004288	Request	Server Side Code Injection	MEDIUM	HIGH
Java code injection com.opensymphony (Header)	200003471	Request	Server Side Code Injection	HIGH	HIGH
Java code injection com.opensymphony (Parameter)	200003470	Request	Server Side Code Injection	HIGH	HIGH
Java code injection com.opensymphony (URI)	200003472	Request	Server Side Code Injection	HIGH	HIGH
JBOSS admin panel URL 3	200010106	Request	Predictable Resource Location	MEDIUM	MEDIUM
JSP Expression Language Expression Injection (URI)	200004281	Request	Server Side Code Injection	LOW	HIGH
Object Graph Navigation Library Expression Injection (URI)	200004280	Request	Server Side Code Injection	LOW	HIGH

上記の CVE 番号 (CVE-2017-5638) は、Apache Struts2 の脆弱性に対応したシグネチャー一覧であることを表示しています。Adv.WAF では、1 つの CVE 番号に関連したシグネチャが複数存在していることがあります。

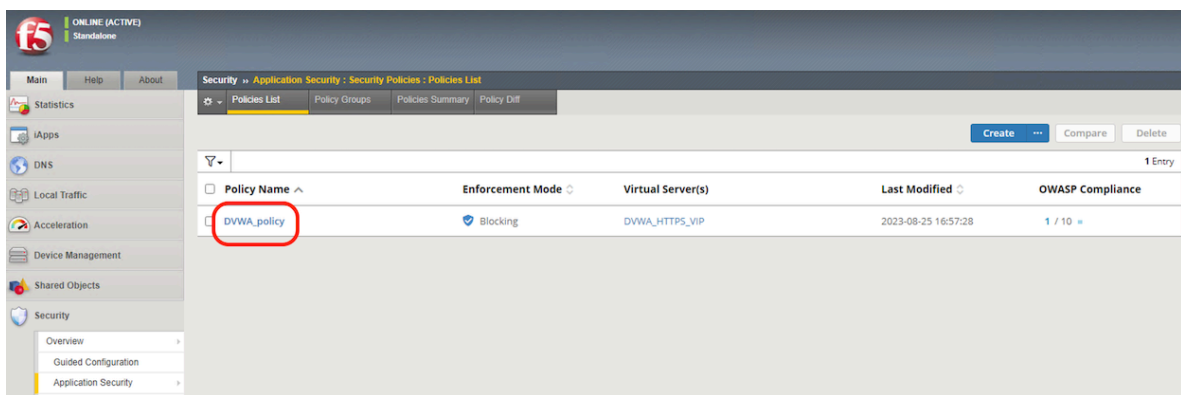
2.1.15 Geolocation の設定

Geolocation Enforcement 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。(F5 ハンズオンでは設定画面の確認のみとなります。)

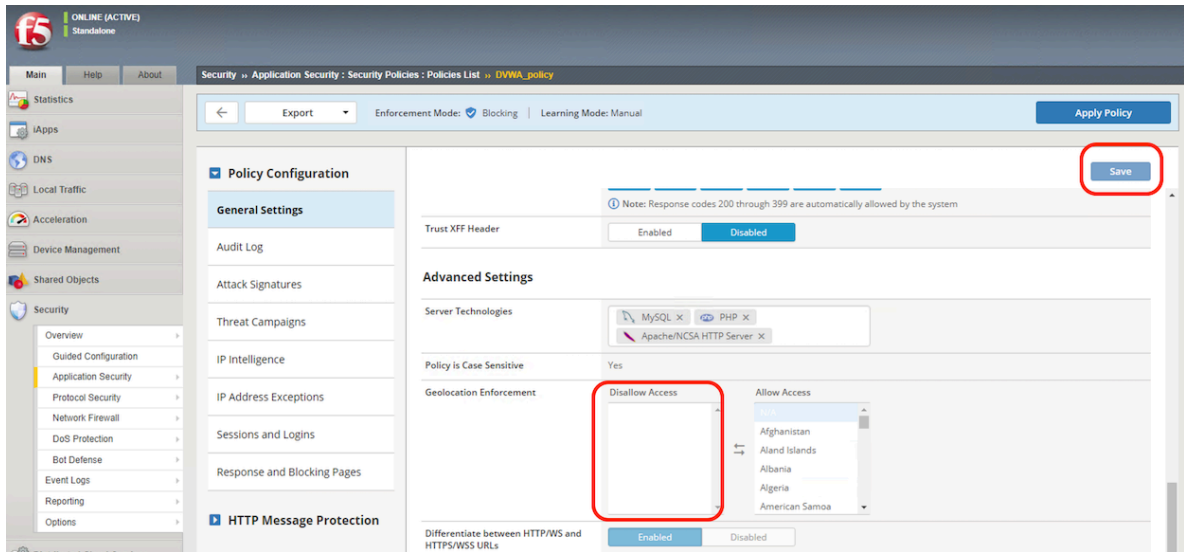
1. **Security >> Application Security : Policy Building : Learning and Blocking Settings の IP Addresses/Geolocations** において、**Access from disallowed Geolocation** の Learn/Alarm/Block がチェックされていることを確認します。



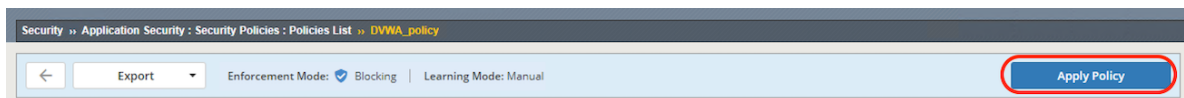
2. **Security >> Application Security : Security Policies : Policies List** にて、対象のポリシーを選択します。



3. **General Setting の Geolocation Enforcement **** にて、接続する予定のない国を ****Disallow Access** に移動し、**Save** を押します。



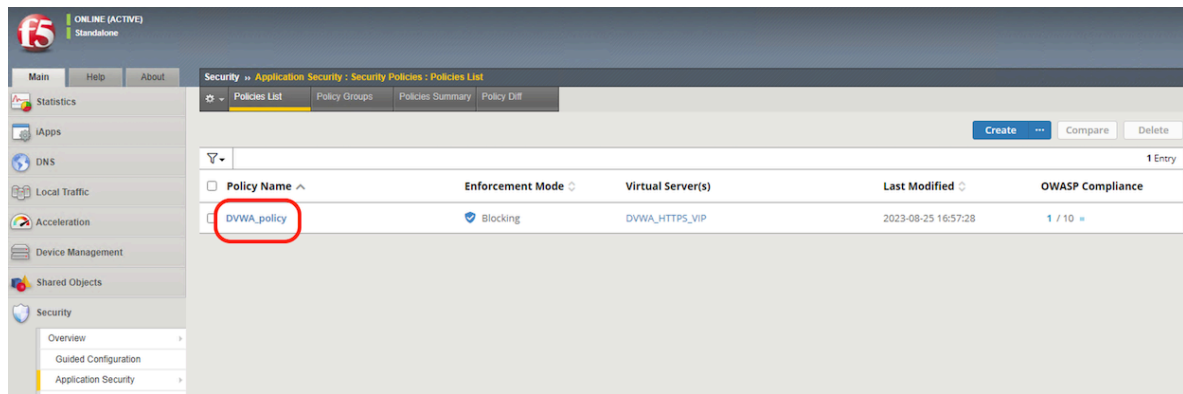
4. *Apply Policy* を押します。



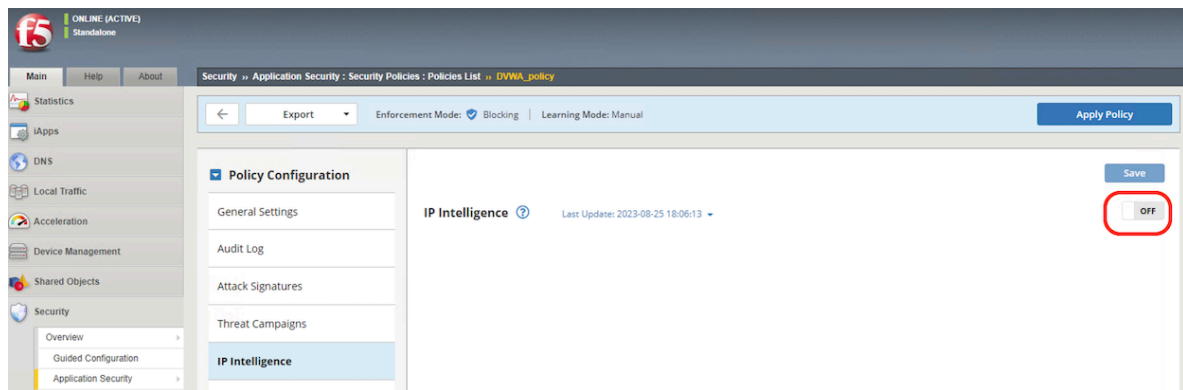
2.1.16 IP Intelligence (IPI) の設定

IP Intelligence を設定することで、既知の悪意ある IP アドレスからの攻撃を Block することが可能です。Application Security 処理の前段で IP アドレスの評価が行われるため、CPU 負荷高騰を和らげる効果があります。WAF と L7DDoS において IP Intelligence を利用することが可能です。(F5 ハンズオンでは設定画面のみの確認となります。)

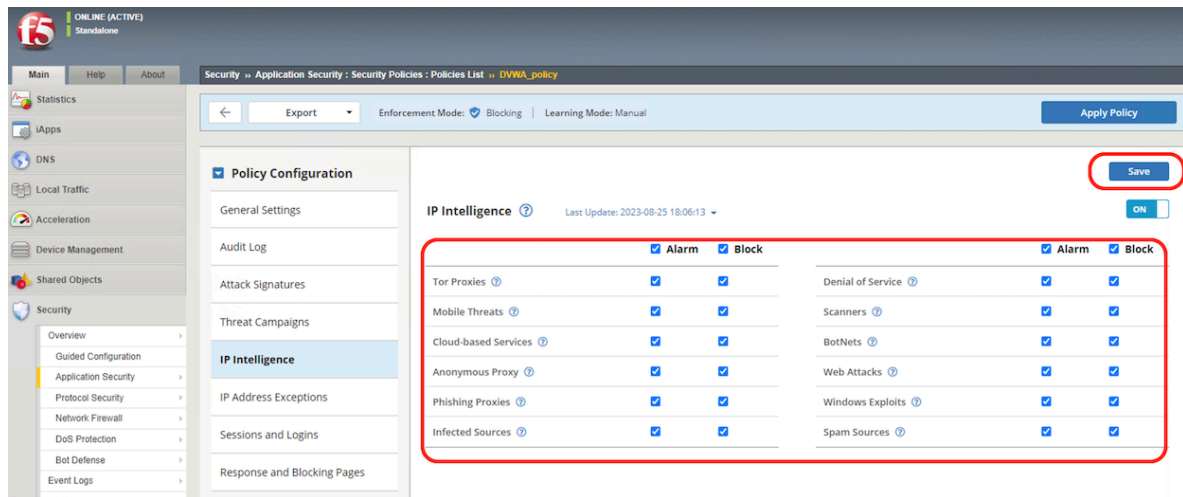
1. **Security >> Application Security : Security Policies: : Policies List** にて、対象のポリシーを選択します。



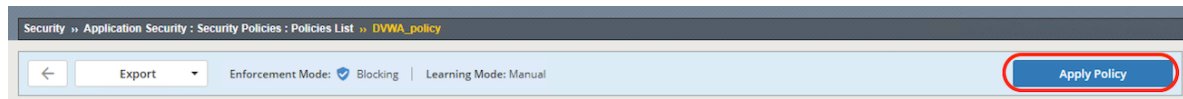
2. IP Intelligence を On にします。



3. チェックしたいカテゴリの Alarm または Block にチェックを入れます。その後、Save を押します。



4. *Apply Policy* を押します。



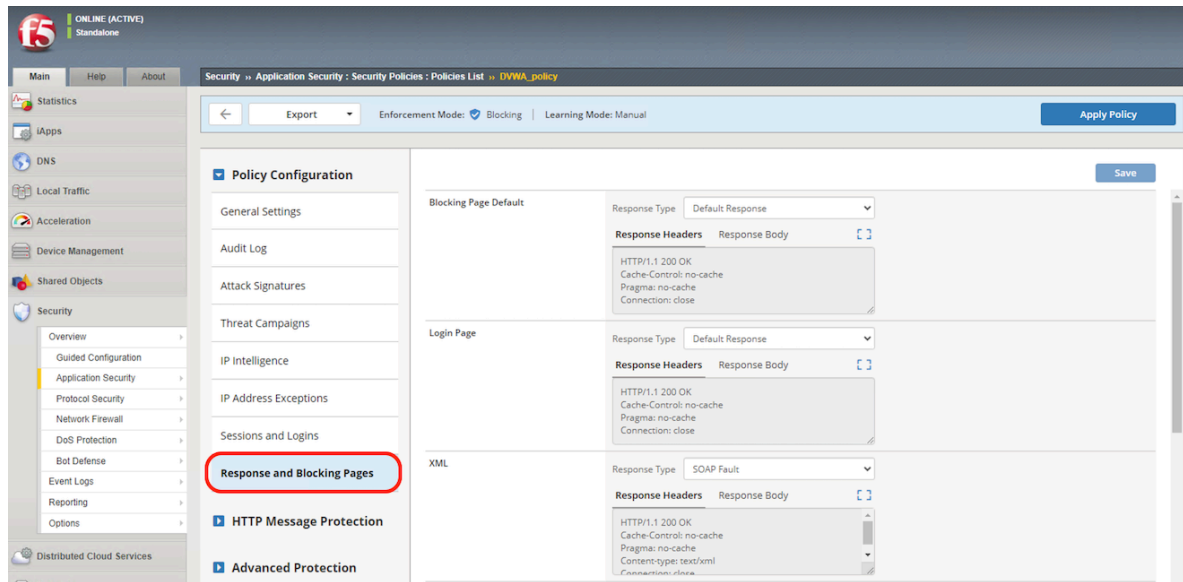
注釈: 上記の他、L7DoS Shun と IP Intelligence を組合せることによって、IP Intelligence の IP レピュテーション DB のリストを L7DoS 対策の Shun list(Auto-blacklisting) として利用が可能です。

IP Intelligence を利用するには、別途サブスクリプションライセンスが必要となります。

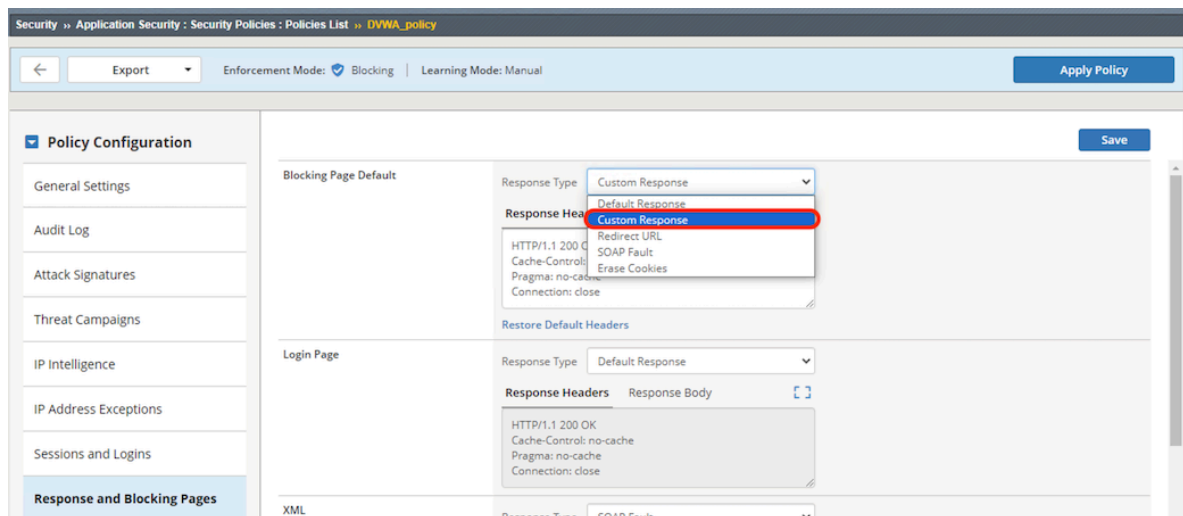
2.1.17 Blocking モード画面のメッセージカスタマイズ

攻撃をブロックした際にユーザに返されるレスポンスページの内容を変更することが可能です。(必須ではありません。)

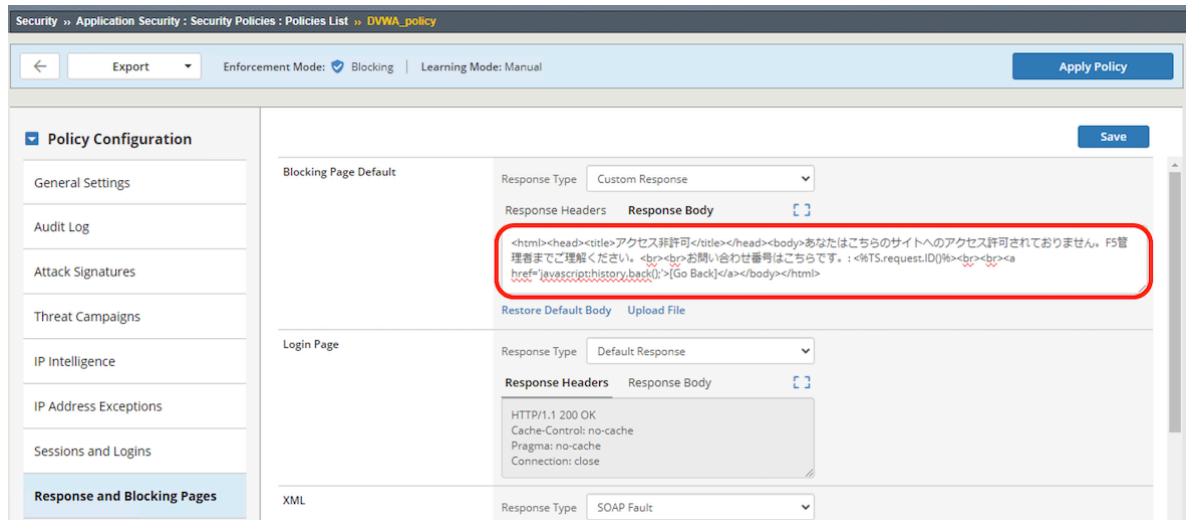
1. **Security >> Application Security : Security Policies : Policies List >> ポリシー名** において、**Response and Blocking Pages** を選択すると以下が表示されます。



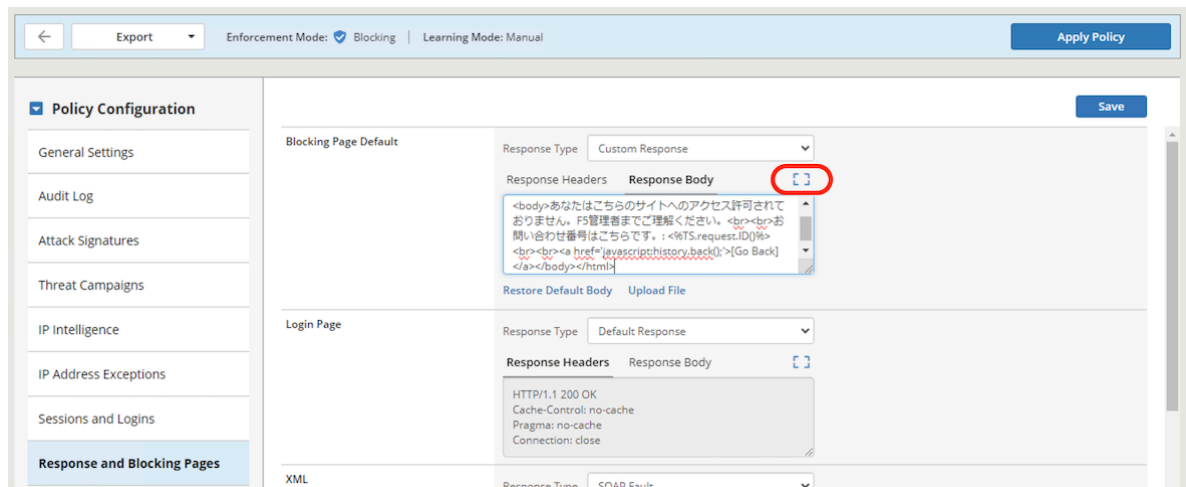
2. Response Body タブにて、Custom Response を選択します。



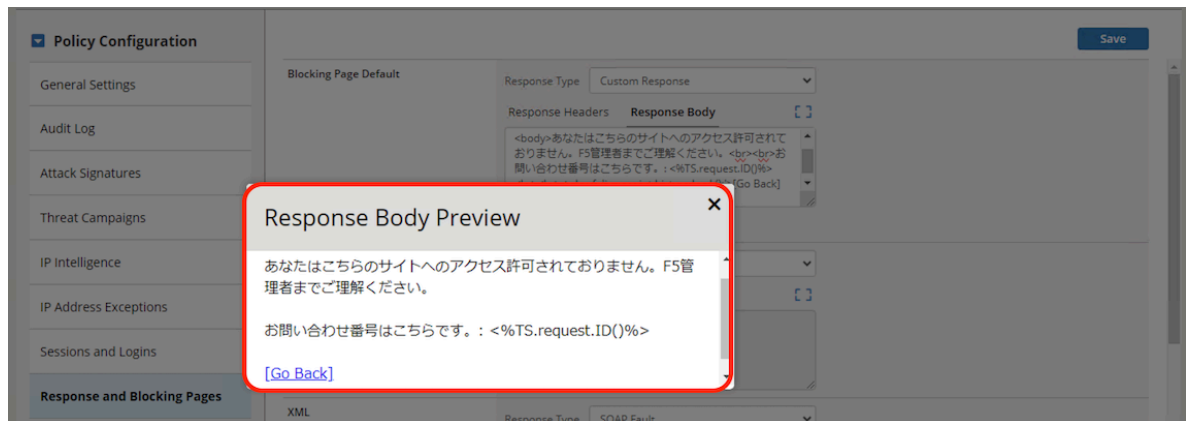
3. Response Body において、表示させたいメッセージに変更します。



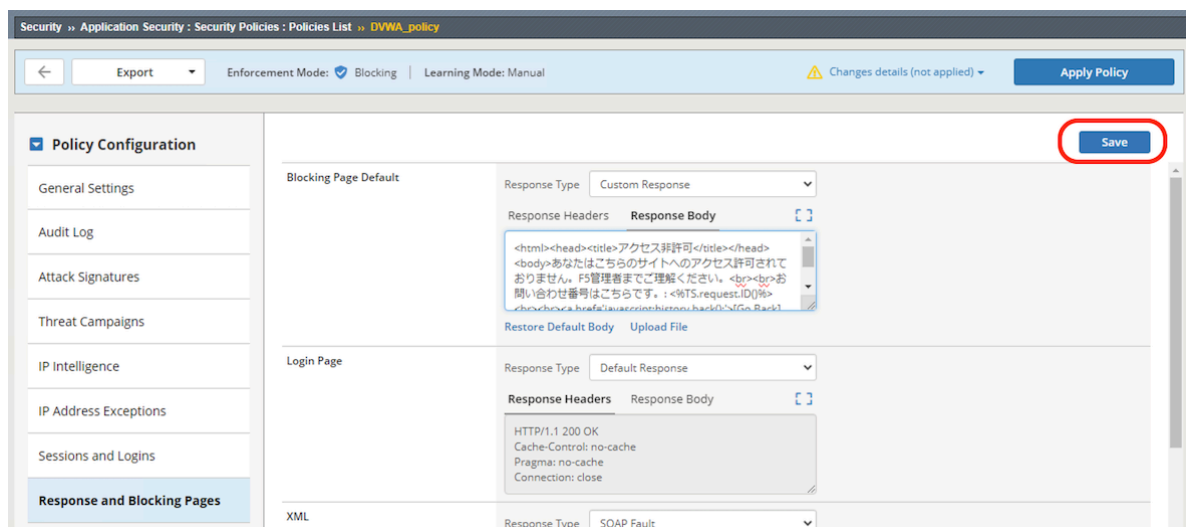
4. 右上の枠のようなボタンを押します。



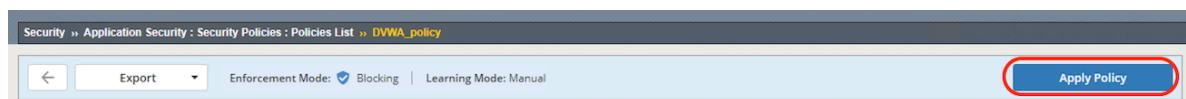
5. ブロックページのレビューが表示されます。



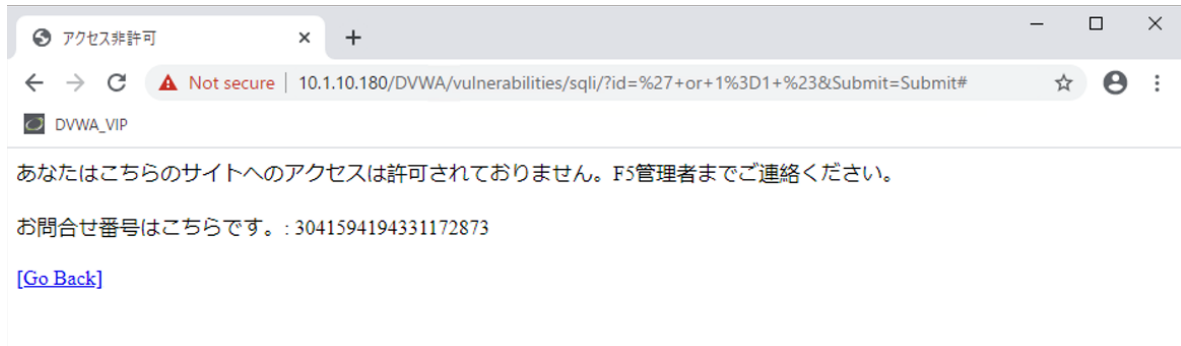
6. メッセージが表示させたい内容と一致していれば、**save** を押します。



7. **Apply Policy** を押します。



8. Windows Client にて、再度 SQL インジェクション攻撃を行います。ブロックメッセージが変更されていることを確認します。



2.2 AWAF 設定中級編

Comming soon!