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 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

ディ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 でご確認下さい。

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。

(5	BIG-IP Configuration Utility F5 Networks, Inc.
Username admin	Your password has expired. Please change it using the fields on the left.
Current Password	

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。



3. Next ボタンを選択します。

ß	ONLINE (ACTIVE) Standalone Provisioning Warning		
Mair	h Help About	Setup Utility » Introduction	
🚺 Se	tup Utility	Welcome	
	Introduction		
	License	Satus Utility	
	Resource Provisioning	To begin configuring this BIG-IP® system, please complete the Setup Utility. To begin, click the *Next* button.	
	Device Certificates		
	Platform	Next	
	Network		
	Redundancy		
	VLANs		
	NTP		
	DNS		
	ConfigSync		
	Failover		
	Mirroring		
	Active/Standby Pair		
	Discover Peer		

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。

in Help About	Setup Utility » License	
etup Utility	General Properties	
Introduction	License Type	Evaluation
License	Licensed Date	Sep 25, 2020
Resource Provisioning	License Expiration Date	Nov 10, 2020
Device Certificates Platform		Advanced Web Application Firewall, VE-1G (PTJVEAJ-MUSTHAP) Rate Shaping
Network		SSL, VE Max Compression, VE
Redundancy	Active Modules	 Exclusive Version, v13.1.X - 18.X IP Intelligence, 3Yr, VE-1G/VE-3G/VE-5G(Subscription) (YXHJYOC-GTMTTFF)
VLANs		 Subscription expires after Nov 10, 2020 Threat Campaigns, 3Yr, VE-1G(Subscription) (QCBHGIM-ZGBAJSG)
NTP		 Subscription expires after Nov 10, 2020
DNS		
ConfigSync		Advanced Firewall Manager, VE-1G Advanced Policy Manager, VE, 1Gbps
Failover		Advanced Protocols, VE Anti-Bot Mobile, VE 1 Gbps
Mirroring		APM, Base, VE (50 CCU / 200 AS) App Mode (TMSH Only, No Root/Bash)
Active/Standby Pair		BIG-IP VE, Multicast Routing External Interface and Network HSM, VE
Discover Peer	Optional Modules	IP Intelligence, 1Yr, VE-1G/VE-3G/VE-5G ITM ADD-VE 1G
		Routing Bundle, VE Secure Web Gateway, VE-25M-1G, 500 Sessions, 1Yr Secure Web Gateway, VE-25M-1G, 500 Sessions, 3Yr Threat Campaigns, 1Yr, VE-1G URL Filtering, VE-25M-1G, 500 Sessions, 3Yr URL Filtering, VE-25M-1G, 500 Sessions, 3Yr VE SSL Compression Offload, Low
	Inactive Modules	

ß	ONLINE (AC Standalone Provisioning	TIVE) 9 Warning	The chart is now showing the minimum resources required for the selected modules Click Revert to again show the current resource allocation						
Main	Help	About	Setup Utility » Resource Pr	ovisioning					
I Set	tup Utility								
	Introduction		Modified Resource Allocation	(prior to redistr	ibution)				
	License		CPU	MGMT	TMM(89%)				
	Resource Provisio	ning	Disk (35GB)	ASM			Unallocate	d	
	Device Certificates	5	Memory (7.7GB)	MGMT	ТММ	ASM	Unallocated		
	Platform		Module		Provisioning	License Status		Required Disk (GB)	Required Memory (MB)
	Network		Management (MGMT)		Small	• N/A		0	1264
	Redundancy		Local Traffic (LTM)		None	📰 Unlicensed		0	1856
	VLANs		Application Security (AS)	0	Nominal	✓ Eicensed		20	1492
	NTP		Application Security (Adv		None			12	544
	DNS		Fraud Protection Service	(FPS)	None	Line Line			449
	ConfigSync		Global Traffic (DNS)		□ None	Onicensed		0	140
	Mirroring		Link Controller (LC)		None	Unlicensed		0	148
	Active/Standby F	Pair	Access Policy (APM)		None	Limited mode a	vailable without a license	12	494
	Discover Peer		Application Visibility and I	Reporting (AVR)	None	ticensed 📷		16	576
			Policy Enforcement (PEN	1)	None	Unlicensed		16	1223
			Advanced Firewall (AFM)		None	Unlicensed		16	1058
				Janagar (AAM)	None	Unlicensed		32	2050
				vialitagel (Avrivi)	None	E Unlicensed		24	4096
			Secure Web Gateway (SI	WG)				2.4	7000
			iRules Language Extension	ons (iRulesLX)	U None	E Licensed		U	748
			URLDB Minimal (URLDB)	None	Unlicensed		36	2048
			SSL Orchestrator (SSLO))	None	Unlicensed		0	128
			Carrier Grade NAT (CGN	AT)	None	E Unlicensed		16	336
			Back Revert Next						

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。

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。

Standalone		
tain Help About	Setup Utility » Device Certi	ficates
Setup Utility	General Properties	
Introduction	Name	server.crt
License	Certificate Subject(s)	localhost.localdomain, MyCompany
Resource Provisioning	Certificate Properties	
Diatform	Public Key Type	RSA
Plauorm	Public Key Size	2048 bits
Network	Expires	Sep 23 2030 02:12:02 PDT
Redundancy	Version	3
VLANs	Serial Number	95:9f:b9:84:03:d7:a5:96
NTP	Fingerprint	SHA256/B7:FC:C0:16:77:04:50:51:9C:62:5F:B0:9E:B8:B5:89:97:F5:BA:55:1C:C1:FA:84:CD:6A:41:D5:F4:A7:CD:26
DNS		Common Name: localhost.localdomain
ConfigSync	Subject	Organization: MyCompany Division: MyOrg
Failover	outjeet	Locality: Seattle State Or Province: WA
Mirroring		Country: -
Active/Standby Pair		Self
Discover Reer	Email	root@localhost.localdomain
51350701 1 001	Subject Alternative Name	

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。)

ONLINE (A Standalone	CTIVE)	Activation Complete Configure your platform.	
Main Help	About	Setup Utility » Platform	
Setup Utility			
Introduction		General Properties	
Introduction		Management Config IPV4	Automatic (DHCP) Manual
License		Management Config IPV6	Automatic (DHCP) Manual
Resource Provisi	oning	Host Name	big80.f5jp.local
Device Certificate	9S	Host IP Address	Use Management Port IP Address V
Platform		Time Zone	Japan V
Redundancy			
Reduitdancy		User Administration	
VLANs			
NTP		Root Account	Password:
DNS			Confirm:
ConfigSync		SSH Access	Z Enabled
Failover		SSH IP Allow	* All Addresses 🗸
Mirroring		Back Next	
Active/Standby	Pair		
Discover Peer			

9. Finished ボタンを選択します。

ONLINE (ACTIVE) Standalone					
Main Help About	Setup Utility » Network				
Setup Utility					
Introduction	Standard Network Configuration				
License					
Resource Provisioning	Redundancy VI ANs				
Device Certificates	• NTP				
Platform	Config Sync Failover Mirroring Pose Davice Discourse (for Redundant Configurations)				
Network					
Redundancy					
VLANs	Next				
NTP					
DNS	Advanced Network Configuration				
ConfigSync	Finished for the Configurations by clicking Finished and navigating to the Main tab of the Configuration Utility.				
Failover					
Mirroring					
Active/Standby Pair					
Discover Peer					

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。

CONLINE (ACTIVE) Standalone		
Main Help About	Network » VLANs : VLAN List	t » New VLAN
Ma Statistics		
_	General Properties	
iApps	Name	external
Local Traffic	Description	
Acceleration	Тад	
Device Management	Resources	
Shared Objects		Interface: 1.2 V Tagging: Untagged V
Security	Interfaces	1.1 (untagged)
Retwork		
Interfaces		Edit
Routes 📀		
Self IPs 🕒	Configuration: Basic V	
Packet Filters	Source Check	
Quick Configuration	MTU	1500
Trunks	sFlow	
Tunnels	Polling Interval	Default V
Route Domains 🔶	Sampling Rate	Default V
VLANs >		
Service Policies	Cancel Repeat Finished	

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。

AWAF v17.1 セットアップガイド

Standalone	CONLINE (ACTIVE) Standalone				
Main Help About	Network » VLANs : VLAN Li	ist » New VLAN			
Mage Statistics	General Bronarties				
iApps	Name	Internal			
Local Traffic	Description				
Acceleration	Tag				
Device Management	Resources				
Shared Objects		Interface: 1.1 V Tagging: Untagged V Add			
Network	Interfaces	1.2 (untagged)			
Interfaces		Edit Delete			
Routes					
Self IPs 📀	Configuration: Basic V				
Packet Filters	Source Check				
Quick Configuration	MTU	1500			
Trunks	sFlow				
Tunnels	Polling Interval	Default V			
Route Domains 🔶	Sampling Rate	Default V			
VLANs >					
Service Policies	Cancel Repeat Finished				

12. 以下のようになります。

CONLINE (ACTIVE) Standalone				
Main Help About	Network » VLANs : VLAN List			
Mag Statistics	VLAN Groups			
iApps	• Search			Create
Local Traffic	✓ ▲ Name	Application Tag	Untagged Interfaces Tagged	Interfaces
	external	4094	1.1	Common
Acceleration	internal	4093	1.2	Common
Device Management	Delete			

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

Standalone		
Main Help About	Network » Self IPs » New Sel	fIP
Ma Statistics		
_	Configuration	
iApps	Name	external-selfip
Local Traffic	IP Address	10.1.10.80
Acceleration	Netmask	255.255.255.0
	VLAN / Tunnel	external V
Device Management	Port Lockdown	Allow None
bhared Objects	Traffic Group	Inherit traffic group from current partition / path
C Recently	-	traffic-group-local-only (non-floating)
Security	Service Policy	None 🗸
Network	Cancel Repeat Finished	

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

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。

Standalone		
Main Help About	Network » Self IPs » New Self	'IP
Magazine Statistics		
_	Configuration	
iApps	Name	internal-selip
Local Traffic	IP Address	10.1.20.80
Acceleration	Netmask	255.255.255.0
	VLAN / Tunnel	internal 🗸
Device Management	Port Lockdown	Allow Default
🐞 Shared Objects	Traffic Group	Inherit traffic group from current partition / path
Security		
V occurry	Service Policy	None 🗸
Network	Cancel Repeat Finished	·

15. 以下のようになります。

ONLINE (ACTIVE) Standalone					
Main Help About	Network » Self IPs				
Mag Statistics	🔅 🚽 Self IP List				
iApps	ŀ	Search			Create
Local Traffic	V 🕈 Name	Application P Address	Netmask VLAN / Tunnel	Traffic Group	Partition / Path
	external-selfip	10.1.10.80	255.255.255.0 external	traffic-group-local-only	Common
(Acceleration	internal-selip	10.1.20.80	255.255.255.0 internal	traffic-group-local-only	Common
Device Management	Delete				

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。

ONLINE (ACTIVE) Standalone		
Main Help About	Network » Routes » New Rou	rte
Ma Statistics		
_	Properties	
iApps	Name	Default-GW
Local Traffic	Description	
Acceleration	Destination	0.0.0.0
Device Management	Netmask	0.0.0
	Resource	Use Gateway 🗸
Nared Objects	Gateway Address	IP Address V 10.1.10.1
Security	MTU	
Retwork	Cancel Repeat Finished	

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。)

CONLINE (ACTIVE) Standalone				
Main Help About	Network » Routes » New Rou	rte		
Magazina Statistics				
_	Properties			
iApps	Name	Servers-Route		
Local Traffic	Description			
Acceleration	Destination	10.1.100.0		
Device Management	Netmask	255.255.255.0		
_	Resource	Use Gateway 🗸		
Nhared Objects	Gateway Address	IP Address 10.1.20.1		
Security	MTU			
Retwork	Cancel Repeat Finished			

18. 以下のようになります。

ONLINE (ACTIVE) Standalone								
Main Help About	Network » Routes							
Mage Statistics	🚓 👻 Route List							
iApps								Add
Local Traffic	Vame	Application	Destination	Netmask	Route Domain	Resource Type	Resource	Partition / Path
Acceleration	Default-GW		Default IPv4		Partition Default Route Domain	Gateway	10.1.10.1	Common
_								

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。

system » Configuration : De	vice : DNS
🌣 🚽 Device 🗸 👻	OVSDB App IQ
operties	
NS Lookup Server List	Address: Add 10.1.1.2
	Edit Delete Up Down
BIND Forwarder Server List	Address:
	Edit Delete Up Down
	Address:
DNS Search Domain List	Add
	Edit Delete Up Down
NS Cache	
Version	

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。

Syste	System » Configuration : Device : NTP							
÷.	Device	- C	OVSDB	App IQ				
Prope	r ties Server List		Address: ntp.n Add ntp.nict.jp	ict.jp				
			Edit Delet	e				
Upda	te							

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。

ſ	ONLINE (AC Standalone	TIVE)		
Mai	in Help	About	Local Traffic » Virtual Servers : Virtual Server List	
Maga S	tatistics		Image: The server List Virtual Address List Statistics	
i4	Apps		Search	Create
D L	ocal Traffic		Status Aname Description Application Destination Service Port Type Resources Partition	on / Path
Network Map			No records to display.	
	Virtual Servers	+	Enable Disable Delete	
	Policies	+		

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 Pofile(Client) にて clientssl を選択します。

AWAF v17.1 セットアップガイド

Main Help About	Local Traffic » Virtual Servers	: Virtual Server List » New Virtual Server				
And Statistics						
	General Properties					
iApps	Name	DVWA_HTTPS_VIP				
Local Traffic	Description					
Network Map	Туре	Standard				
Virtual Servers	Source Address	Host Address List				
Policies Profiles	Destination Address/Mask	Host Address List 10.1.10.180				
Ciphers	Service Port					
Pools	Notify Status to Virtual Address					
Nodes	State	Enabled V				
Monitors (+)	Configuration: Basic V					
Traffic Class (+)	Protocol	TCP V				
Address Translation	Protocol Profile (Client)	tcp 🗸				
	Protocol Profile (Server)	(Use Client Profile)				
Acceleration	HTTP Profile (Client)	http V				
Device Management	HTTP Profile (Server)	(Use Client Profile) V				
	HTTP Proxy Connect Profile	None				
Nared Objects	FTP Profile	None 🗸				
Security	PPTP Profile	None V				
Network	SSL Profile (Client)	Selected Available /Common /Common clientssl-insecure-compatible clientssl-secure clientssl-secure clientssl-secure clientssl-secure clientssl-secure				
		wom-default-clientss				

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

Service Frome	Inone V
SMTP Profile	None 🗸
VLAN and Tunnel Traffic	All VLANs and Tunnels V
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。

ONLINE (ACTIVE) Standalone		
Main Help About	Local Traffic » Pools : Pool Li	ist » New Pool
Statistics	Configuration: Basic	
iApps	Name	DVWA_HTTP_Pool
Local Traffic	Description	
Network Map Image: Compare the second seco	Health Monitors	Active Available Common gateway_icmp << >> http http http2 http2_head_f5 http.ead_f5 http.ead_f5 http2_head_f5 http2_head
Profiles	.	
iBulas	Load Balancing Method	Round Robin
Rules	Priority Group Activation	
Nodes Image: Second s	New Members	New Node O New FQDN Node Node Name: Address: 10.1.20.202 Service Pont 80 HTTP
Acceleration Device Management		Node Name Address/FQDN Service Port Auto Populate Priority 10.1.20.202 10.1.20.202 80 0 Edit Delete
🔥 Shared Objects	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 +	
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。)

ONLINE (ACTIVE) Standalone				
Main Help About	Security » Guided Configuration			
Statistics			Ver	rsion: 6.0 1 Upgrade Guided Configuration
iApps	Web Application	API Security	Mobile Protection	
Local Traffic	Protection	,	_	
Acceleration		O		
Device Management			Coming Soon!	
Nared Objects				
Security	Configurations			
Overview Guided Configuration	Import			Filter Configurations by Name
Application Security	Status	Name 🔺	Туре	
Protocol Security				
Network Firewall				
DoS Protection				
Bot Defense				
Cloud Services				
Event Logs >				
Reporting				
Options				
Network				
System				

 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			Product Version			
Guided Configuration		\sim	10.0			\sim
Select a product container						
Name ↑↓	Туре ↑↓	Date ↑↓		Description $\uparrow \downarrow$		
Guided_Configuration	Release	Mar 15, 2	023	Guided_Configuration		
Select a download file						
File Name ∱↓		Description			Size	
f5-lappslx-agc-usecase-pack-10.0-0.0.1636.tar.gz		Access and Advanced WAF Guided Configuration 10.0		10 MB		
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		
relnote-guided-config-10-0.html		Guided Configuration 10.0 release note		86 KB		
reinote-guided-config-10-0.html.md5		Guided Configuration	on 10.0 release note		66 Bytes	

3. 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。

Main Help About	scurity » Guided Configuration	
Mage Statistics	Varsion: 6.0.0 Lloorada Ouidad Configuratio	<u>on</u>
iApps Local Traffic Acceleration	Web Applica Protectio Upgrade Guided Configuration To begin installation you have to download a use case pack(.tar.gz) file from downloads.f5.com(Guided Configuration). Once downloaded you can upload the use case pack below.	
Device Management Shared Objects Security	Import Guided Configuration Use Case Pack Choose File No file has been chosen	
Overview Guided Configuration	Upload and Install	
Application Security	Status Name A Type	
Network Firewall		

4. インストールしている途中のイメージです。

Standalone	
Main Help About Security » Guided Configuration	
Statistics	Version: 6.0.0 Upgrade Guided Configuration
Web Applica Protectio Upgrade Guided To begin installation you have to downloads.f5.com(Guided Configuration). Or	Configuration ad a use case pack(.tar.gz) file from ice downloaded you can upload the use
Acceleration Case pack I Device Management Uploading file to	o the server
Security Configuration	
Overview Import Import Guided Configuration Use Case Pack Guided Configuration Import Import Guided Configuration Use Case Pack	
Application Security > Status Upload and	Install
Protocol Security Network Firewall	
DoS Protection > Bot Defense >	

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。

Standalone						
Main Help About	Security » Guided Configuration	I				
Mage Statistics					Version: 7.0 @ Upgrade Guide	d Configuration
iApps	Web Application Protection	API Security Protection	Dos Protection	Bot Protection	Mobile Protection	
Acceleration		6		A		
Device Management		**		•	Coming Soon!	
Shared Objects						
Security						
Overview	Web Application Prote	ection				
Guided Configuration						
Application Security	Web Application Com	prehensive Protection	Web Application F	Protection	Traffic Security Policy	
Protocol Security	Configure Application Compr	ehensive Protection	Configure Application Pr	otection Configuration using Virtual	Configure rules to protect traffic by different	ASM policies
Network Firewall	Configuration using Virtual Se	uver.	Server		based on matching conditions	
DoS Protection						
Bot Defense						
Cloud Services	Configurations					
Event Logs	Incort					
Reporting	Import				Filter Configurations by Name	

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。



 5. 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		
le		
Security Policy	Virtual Server	Summary
		Cumuna, y
Web Application Security	Policy Properties	Hide Advanced Setting
Security Policy Name		
DVWA_policy		
Transparent O Blocking		
Select type of policy to protect application		
Generic Application Specific		
Application Language 0		
Unicode (utf-8)	~	
Server Technologies		
Available	Selected	
Filter	Дра	che/NCSA HTTP Server
AngularJS	(I) Nys	QL
Apache Struts		,
Apache Tomcat		
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 Virtul Server を右に移動させ、*Save* & *Next* ボタンを押します。

Security » Guided C	Configuration			
Web Application Prot	ection Configuration :DVWA_policy NOT DEPLOYE			
<u>@</u>			0	
	Security Policy	Virtu	ial Server	Summary
Virtual Se	erver Properties			
Assign Policy to	virtual Server(s)			
Virtual Server				
○ Create New	Use Existing			
Assign Virtual	Servers			
Available			Selected	
Filter		T	/Common/DVWA_HTTPS_VIP	
No available ite	ms	•		
Cancel Sa	ve Draft Back Save & Next			

11. 内容を確認し、Deploy ボタンを押します。
| Security » Guided Configuration | | | | | | |
|---------------------------------|--|---|-------|--|--|--|
| Web Ap | plication Protection Configuration : | | | | | |
| <u>@</u> | — | | | | | |
| | Security Policy | Virtual Server Summary | | | | |
| | | | | | | |
| Vou | r application is ready | to be deployed | | | | |
| TOU | r application is ready | to be deployed. | | | | |
| The ap | oplication is correctly configured, an | id ready to be deployed. Review the summary. You can click 🖋 on any step to make changes. | | | | |
| | | | | | | |
| Sumr | nary | | | | | |
| U | Security Policy - | | San A | | | |
| | | | | | | |
| | Security Policy Name | DVWA_policy | | | | |
| | Type of policy to | Generic | | | | |
| | protect application | | | | | |
| | Enforcement Mode | Transparent | | | | |
| | | I biende (uif 0) | | | | |
| | Application Language | Unicode (ut-o) | | | | |
| | Server Technologies | Apache/NCSA HTTP Server, 🔪 MySQL, 🐵 PHP | | | | |
| | | | | | | |
| | Trust XFF Headers | Disabled | | | | |
| 2 | | | | | | |
| Q | Virtual Server | | (AP) | | | |
| Corre | ol Court Draft Draft | | | | | |
| Gane | Save Dratt 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) Standalone Live Updates Available				
Main Help About	Security » Overview : Summar	y		
Statistics	🚓 👻 Summary Analy	tics Application - Protocol	DoS I OWASP Compliance Dashbo	bard
iApps	Attach •	Detach 🔹 Create 🔹		Slocking 🔿 Transparent 😲 Disabled 🚫 Detached
Con Local Traffic	DoS Profile			
Acceleration	Bot Defense Profile	Protection → Bot Defense → Application S	ecurity Learn More	Compact Detailed
Device Management	Security Policy	les and policies		1 Entry
Device management	Logging Profile	DoS Protection 🟹	Bot Defense 🟹	Application Security 🟹
Nared Objects				
Security	DVWA_HTTPS_VIP	\otimes	0	O DVWA_policy
Overview				
Guided Configuration				
A				

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

ONLINE (ACTIVE) Standalone Live Updates Available			
Main Help About	Security » Overview : Summary		
Statistics	🌣 🛪 Summary Analytics Application 👻 P	rotocol DoS 💌 OWASP Compliance	Dashboard
і Арря	Attach - Detach - Crea	ite 🔹	Slocking 🔿 Transparent 🔋 Disabled 🚫 Detached
Local Traffic	Choose a Logging Profile to attach to the selected virtual serv		
Acceleration	A new Logging Profile will be added to the existent one(s)	pplication Security Learn More	Compact Detailed
Device Management	Q. Search logging profile		1 Entry
Nared Objects	Log all requests	Bot Derense V	Application security V
Security	Log illegal requests local-bot-defense	Ø	
Overview	local-dos		
Guided Configuration	10121 005		
Application Security	Attach Cancel		
Protocol Security			
Network Firewall			

14. Local Traffic >> Virtual Servers: Virtual Server List にて作成済みの Virtul 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。

I ONLINE (ACTIVE) Standalone Live Updates Available							
Main Help About Local Traffic » Virtual Servers : Virtual Server List » DVWA_HTTPS_VIP							
Mage Statistics	🗱 🗸 Properties Reso	ources Security Statistics					
iApps	Policy Settings						
Local Traffic	Destination	10.1.10.180:443					
Network Map	Service	HTTPS					
Virtual Servers	Application Security Policy	Enabled Policy: DVWA_policy					
Policies	Service Policy	None					
Profiles	IP Intelligence	Disabled V					
Ciphers	DoS Protection Profile	Disabled V					
iRules	Bot Defense Profile	Disabled V					
Pools	Application Cloud Security	Disabled V					
Nodes	Services	Enabled v					
Monitors 📀		Selected Available					
Traffic Class	Log Profile	/Common /Common Log illegal requests					
Address Translation		Solan-retwork local-bot-defense local-dos					
Acceleration	Update	· · · · · · · · · · · · · · · · · · ·					

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。

ONLINE (ACTIVE) Standalone		
Main Help About	Security » Application Security : Policy Building : Learning and Blocking Settings	
Statistics	Contraction of the second section of the second section of the second section of the second section of the second	
iApps	O DVWA_policy	Apply Policy
S DNS	Dallay Duilding Settings Constrict Dallay Duilding Cattings	Nate: Olide Save to rate a set of same you made on this same Direction Cations
Fin Local Traffic	Promy burning settings Search in Policy burning Settings	Note: Citck Save to retain any changes you made on bits screen. Divoking Settings
	▶ Antivirus	
Acceleration	Attack Signatures	
	CSRF Protection	
Device Management	Content Profiles	
Shared Objects	▶ Cookies	
	▼ Data Guard	
Security	Learn Alarm Block Violation	
Overview >	Data Guard: Information leakage detected	
Guided Configuration	► Evasion technique detected ▼ (0 out of 12 subviolations are enabled) ✓ Learn ✓ Alarm ✓ Block	
Application Security >	File Types	
Protocol Security >	▼ General Settings	
Network Firewall		
DoS Protection		
Bot Defense >	Failed to convert character	
Event Logs >	✓ ✓ Illegal HTTP status in response ▼	
Reporting >	□ □ Illegal session ID in URL	
Options >	Request length exceeds defined buffer size -	

16. Apply Policy ボタンを押し、ポリシーを反映させます。

Security » Application Security : Policy Building : Learning and Blocking Settings					
۰ 🕈	Traffic Learning	Learning and Blocking Settings			
	DVWA_policy	 Barning Mode: Manual 	Apply Policy		

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。

Standalone									
Main Help About	Main Help About Security - Application Security : Policy Building : Learning and Blocking Settings								
Market Statistics	🔅 👻 Traffic Learn	ing Learni	ig and Blocking Settings						
I Apps VWA.policy · 🛞 Learning Mode: Manual									
S DNS	Policy Building	Settings S	arch in Policy Building Settings	B	locking Settings Save				
Local Traffic	▶ Antivirus								
Acceleration	▼ Attack Signature	es							
Device Management	Learn A	larm 🗌 Block	Signature Set Name		Signature Set Category				
Device management		Z	PHP Signatures (High/Medium Accuracy) Change signature	properties 🕶	User-defined				
Nared Objects		Z	MySQL Signatures (High/Medium Accuracy) Change signature	properties 🕶	User-defined				
Converte		✓	Apache/NCSA HTTP Server Signatures (High/Medium Accuracy) Change signature	properties 🕶	User-defined				
Security		✓	Generic Detection Signatures (High/Medium Accuracy) Change signature	properties 🕶	Basic				
Overview					Change				
Guided Configuration	Auto-Added Sign	nature Accurac	Medium (also includes signatures with high accuracy)						
Application Security >	Updated Signat	ure Enforcement	t Retain previous rule enforcement and place updated rule in staging 🗸						
Protocol Security >	Note: Newly add	led signatures	re always placed in staging regardless of this setting.						
Network Firewall	Potential False F	Positive Detect	Disabled						
DoS Protection > Apoly Ressource Simanuure for these File Types									
Bot Defense > Add									
Event Logs	Event Logs								
Reporting >									
Options >		-							
Distributed Cloud Services	Delete								

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。

Standalone Live Updates Available				
Main Help About	Security » Application Security : S	Security Policies : Policies List		
Mage Statistics	🔅 🚽 Policies List Policy Gr	roups Policies Summary Policy Diff		
iApps			Create ·	• Compare Export • Delete
Local Traffic	7-			1 Entry
Acceleration	Policy Name A	Enforcement Mode 🔿	Virtual Server(s)	OWASP Compliance
Device Management		🔿 Transparent	DVWA_HTTPS_VIP	0/10
🐞 Shared Objects				
Security				
Overview				
Guided Configuration				
Application Security				
Protocol Security				

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。

Security » Application Security : Security Poli	cies : Policies List » DVWA_policy					
Export Enforce	ement Mode: O Transparent Learning Mode: Manual					Apply Policy
Policy Configuration	♂ 0 Signatures ready to be enforced			Enforce	••• s	itage Disable
General Settings	¥•			1 - 20 of 3080	Entries 1	2 3 4 154 🚺
Audit Log	□ Signature Name and Tag ∧	Signature ID 🗘	Learn	Alarm	Block	Status
Audit Log	Src http: (Header)	200101559	~	~	~	Staging
Attack Signatures	Src http: (Parameter)	200101558	~	~	~	Staging
Threat Campaigns	"/.env" access	200009283	~	~	~	Staging
IP Intelligence	□ D "/.ftpconfig" access	200010137	~	~	~	Staging
	□	200010136	~	~	~	Staging
IP Address Exceptions	□ D "/.idea/" access	200010138	~	~	~	Staging
Sessions and Logins	□ Σ "/.remote-sync.json" access	200010139	~	~	~	Staging
Response and Blocking Pages	□	200010140	~	~	~	Staging
	□ Σ "/.vscode/" access	200010141	~	~	~	Staging
HTTP Message Protection	"/administrator/components/com_comprofiler/" access	200010148	~	~	~	Staging
Advanced Protection	□ 】 "/app_dev.php" access	200010474	~	~	~	Staging
	"/bb_usage_stats/include/bb_usage_stats.php" access	200010149	~	~	~	Staging
	"/cgi/common.cgi" access	200010150	~	~	~	Staging
	□ 🔰 "/es/fcgi-bin/" access	200010151	~	~	~	Staging
	□	200010142	~	~	~	Staging
	□	200010469	~	~	~	Staging
	"/MSD/sql.php" access	200010143	~	~	~	Staging

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。)

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。

AWAF v17.1 セットアップガイド

Main Help About	Security » Event Logs : Loggi	ing Profiles » Create New Logging Profile
Statistics	Logging Profile Properties	Cancel
iApps	Profile Name	Log illegal and staging requests
	Description	
DNS	Application Security	Enabled
Local Traffic	Protocol Security	Enabled
Acceleration	Network Firewall	Enabled
Acceleration	DoS Protection	Enabled
Device Management	Bot Defense	Enabled
Shared Objects Security	Application Security Configuration Basic	
Overview	Storage Destination	Local Storage 🗸
Guided Configuration	Pacio M	
Application Security	Storage Filter Dasic +	Illegal conjusts only
Protocol Security	Request Type	Biocked requests only
Network Firewall	Cancel	lilegal requests, and requests that include staged attack signature or staged threat campaigns or Potential False Positive signature
DoS Protection		All requests
B-10-6		
Bot Detense		

2. Security >> Overview : Summary にて、作成済みの Virtul 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。

ONLINE (ACTIVE) Standalone Live Updates Available					
Main Help About	Security » Overview : Sum	nary			
Statistics	🔅 🚽 Summary Ar	halytics Application	✓ Protocol	DoS 🔊	OWASP Compliance Dashboard
iApps	Attach -	Detach 👻	Create -	🥏 Blocking	🔿 Transparent 😲 Disabled 🛇 Detached
Local Traffic	() Mitigation Flow: Do	DoS Profile(s) Bot Defense Profile(s)	efense \rightarrow Application S	ecurity Learn More	Compact Detailed
During Management	Q Search virtual servers, pr	Security Policy(s)			1 Entry
Shared Objects	Virtual Server ~	Logging Profile(s)	n 🏹 🛛 Bot	Defense 🏹	Application Security $oxed{V}$
Security	DVWA_HTTPS_VIP	\bigtriangledown	\bigtriangledown		 DVWA_policy Log illegal requests
Overview					
Guided Configuration					
Application Security					
Protocol Security					

3. 再度アタッチの設定をします。

ONLINE (ACTIVE) Standalone Live Updates Available				
Main Help About	Security » Overview : Sum	nmary		
Mage Statistics	🔅 🚽 Summary 🛛 A	Analytics Application -	Protocol DoS 🏼	OWASP Compliance Dashboard
iApps	Attach 👻	Detach - Cu	eate 👻 🦁 Blocking	🔿 Transparent 🛛 Disabled 🛇 Detached
Local Traffic	DoS Profile			
Acceleration	Bot Defense Profile	S Protection → Bot Defense -	 Application Security Learn More 	Compact Detailed
Device Management	Security Policy	ofiles and policies		1 Entry
	Logging Profile	DoS Protection 🖓	Bot Defense 🟹	Application Security \bigtriangledown
Shared Objects	DVWA_HTTPS_VIP	\otimes	\otimes	O DVWA_policy
Overview				
Guided Configuration				
Application Security				
Protocol Security				

4. 作成済みの Logging Profile(s) をアタッチします。

ONLINE (ACTIVE) Standalone Live Updates Available									
Main Help About	Security » Overview : Su	mmary							
Main Statistics	🕁 🚽 Summary	Analytics	Application	▼ P	rotocol	DoS 🏾	OWASP Compliance	Dashboard	
iApps	Attach 👻	Detach	•	Crea	ite 👻	🤝 Blocking	🔿 Transparent 🕻	🕽 Disabled 🔇	S Detached
Local Traffic	Choose a Logging Prof	ile to attach to the	selected vir	tual serv	pplication	Socurity Learn Mar		Compact	Detailed
Acceleration	A new Logging Profile	e will be added to th	e existent on	e(s)	pplication	Security Learn Mon	e	Compact	Detailed
Device Management	Q Search logging pro	file			Bo	t Defense 🝸	Applica	tion Security	1 Entry
Nared Objects	Log all requests								
Security	Log illegal and staging	g requests			\Diamond		🗘 DVM	/A_policy	
Overview	Log illegal requests								
Guided Configuration	local-bot-defense								
Application Security	local-dos								
Protocol Security	Attach	Cancel							
Network Firewall									
DoS Protection									
Bot Defense									

2.1.8 シグネチャの動作確認

 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。)

← → C ▲ Not secure 10.1	I.10.180/DVWA/vulnerabilities/sqli/?id=%27+or+1%3D1+%23&Submit=Submit#	☆	θ	:
DVWA_VIP				
	DYWA			
Home	Vulnerability: SQL Injection			
Instructions				
Setup / Reset DB	User ID: Submit			
Brute Force Command Injection	ID: ' or 1=1 # First name: admin Surname: admin			
CSRF	ID: ' or 1=1 #			
File Inclusion	Surname: Brown			
File Upload	ID: ' or 1=1 # First name: Hack			
Insecure CAPTCHA	Surname: Me			
SQL Injection	ID: ' or 1=1 #			
SQL Injection (Blind)	First name: Pablo Surname: Picasso			
Weak Session IDs	ID: ' or 1=1 #			
XSS (DOM)	First name: Bob			
XSS (Reflected)	Sur Home - Smaller			
XSS (Stored)				
C SP Bypass	More Information			
JavaScript	<u>https://www.securiteam.com/securityreviews/5DP0N1P76E.html</u> https://en.wikipedia.org/wiki/SQL_injection			

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。)

AWAF v17.1 セットアップガイド



2.1.9 シグネチャのステージング解除

 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。

	Security	cies : Policies List » DVWA_policy		ala ana ana ana ana ana ana ana ana ana			
Statistics	Export - Enforc	ement Mode: 🔿 Transparent 🕴 Learning Mode: Manual					Apply Policy
iApps						_	
DNS	Policy Configuration	O Signatures ready to be enforced I Signatures have suggestions	(_	Enforce		Stage Dis
Local Traffic		∀ •		Enforce al	l Staged Signa	tures	1 2 3 4 154
Acceleration	General Settings	□ Signature Name and Tag ∧	Signature ID	Learn	Alarm	Block	Status
Device Management	Audit Log	" src http: (Header)	200101559	~	~	~	Staging
Shared Objects	Attack Signatures	structure (Parameter)	200101558	~	~	~	Staging
Security	Threat Campaigns	"/.env" access	200009283	~	~	~	Staging
Overview >	inicat campaigns					-	
Guided Configuration	IP Intelligence	"/.ttpconfig" access	200010137	~	~	~	Staging
Application Security		Image: "/.git/" access	200010136	~	~	~	Staging
Protocol Security	IP Address Exceptions	IMAGE INTERNATIONAL INTERNATIONALIZIA INTERNATIONAL INTERNATIA INT	200010138	~	~	~	Staging
DoS Protection >	Sessions and Logins	"/.remote-sync.json" access	200010139	~	~	~	Staging
Bot Defense	Response and Blocking Pages	V.svn/" access	200010140	~	~	~	Staging
Reporting		Vivscode/" access	200010141	~	~	~	Staging
Options >	HTTP Message Protection	"/administrator/components/com_comprofiler/" access	200010148	~	~	~	Staging
Distributed Cloud Services	Advanced Protection	"/app_dev.php" access	200010474	~	~	~	Staging
Network	Advanced Hotection	"/bb_usage_stats/include/bb_usage_stats.php" access	200010149	~	~	~	Staging
System		Image: "/cgi/common.cgi" access	200010150	~	~	~	Staging
		□ D "/es/fcgi-bin/" access	200010151	~	~	~	Staging
		□ > "/FileZilla.xml" access	200010142	~	~	~	Staging
		□	200010469	~	~	~	Staging
		□ ▶ "/MSD/sql.php" access	200010143	~	~	~	Staging
		"/msd1.24" access	200010152	~	~	~	Staging
		"/myadmin/" access	200010152		1		Staging
		- myounny access	200010133	*	*	*	2105115

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

AWAF v17.1 セットアップガイド

ONLINE (ACTIVE) Standalone			and the second second second second	an a		en la serie da con	
Click to return to the start page							
Main Help About	Security » Application Security : Security Poli	cies : Policies List » DVWA_policy					
statistics	← Export ▼ Enforc	ement Mode: 🔿 Transparent 🕴 Learning Mode: Manual	🔥 Cha	anges details	(not applied)	-	Apply Poli
iApps							
DNS	Policy Configuration	Ø Signatures ready to be enforced Ø 3 Signatures have suggestions Ø			Enforce		Stage D
Local Traffic	Concernal Cottlinger	7.		1	- 20 of 3080	Entries 1	2341
Acceleration	General Settings	Signature Name and Tag ^	Signature ID 🗘	Learn	Alarm	Block	Status
Device Management	Audit Log	src http: (Header)	200101559	~	~	~	Enforced
Shared Objects	Attack Signatures	src http: (Parameter)	200101558	~	~	~	Enforced
Security	Threat Campaigns	V:env" access	200009283	~	~	~	Enforced
Overview		//.ftpconfig" access	200010137	~	~	~	Enforced
Guided Configuration	IP Intelligence						
Protocol Security	IP Address Exceptions	□ D "7.git/" access	200010136	~	~	~	Enforced
Network Firewall		Image: Second	200010138	~	~	~	Enforced
DoS Protection	Sessions and Logins	Image: "/.remote-sync.json" access	200010139	~	~	~	Enforced
Bot Defense >	Response and Blocking Pages	"/.svn/" access	200010140	~	~	~	Enforced
Reporting >		"/.vscode/" access	200010141	~	~	~	Enforced
Options >	HTTP Message Protection	//administrator/components/com_comprofiler/" access	200010148	~	~	~	Enforced
Distributed Cloud Services	Advanced Protection	Image: "/app_dev.php" access	200010474	~	~	~	Enforced
Network	Advanced Protection	Image: "/bb_usage_stats/include/bb_usage_stats.php" access	200010149	~	~	~	Enforced
] System		Image: "/cgi/common.cgi" access	200010150	~	~	~	Enforced
		Image: Second	200010151	~	~	~	Enforced
		FileZilla.xml" access	200010142	~	~	~	Enforced
		Vidx_config/" access	200010469	~	~	~	Enforced
		Image: MSD/sql.php" access	200010143	~	~	~	Enforced
		Imsd1.24" access	200010152	~	~	~	Enforced
		//myadmin/" access	200010153	~	~	~	Enforced
		"/mysql-admin/" access	200010154	~	~	~	Enforced

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。

AWAF v17.1 セットアップガイド



2.1.10 Blocking モードへの変更

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 >> DVWA_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。

Main Help About	Security » Application Security : Security Pol	icies : Policies List » DVWA policy		
Statistics				
	Export • Enfor	cement Mode: 🔿 Transparent 🕴 Learn	ning Mode: Manual	Apply Policy
S webbs				
DNS	Believ Configuration	19		Save
Cocal Traffic	Policy configuration			
Assolation	General Settings	Policy Name	DVWA_policy Partition / Path: Common/DVWA_policy.app	
Acceleration		Description	·	
Device Management	Audit Log	Description	Rapid Deployment Policy	
Shared Objects	Attack Signatures			
Security		Policy Type	Security	
security	Threat Campaigns	Policy Template	Rapid Deployment Policy Learn More	
Overview		Version	2023-08-25 14-55-58	
Application Security	IP Intelligence	(Clain)	Source Host Name: big80.f5jp.local	
Protocol Security	IP Address Excentions		Source Policy Name: /Common/DVWA_policy.app/DVWA_policy	
Network Firewall		Application Language	Unicode (utf-8) 🕥	
DoS Protection	Sessions and Logins	Virtual Server	DVWA_HTTPS_VIP (2*	
Bot Defense				
Event Logs	Response and Blocking Pages	Learning and Blocking		Learning and Blocking Settings 🗹
Reporting		Enforcement Mode		
Options	HTTP Message Protection	chlorcement mode	Transparent Blocking	
Distributed Cloud Services		Policy Building Learning Mode	Automatic Manual Disabled (?)	
2	Advanced Protection	Policy Builder Learning Speed	Fast Medium Slow	
Network				

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。

\leftarrow \rightarrow C \blacktriangle Not secure 10.).1.10.180/DVWA/vulnerabilities/xss_s/	Θ	:
DVWA_VIP			
	DYWA		
Home	Vulnerability: Stored Cross Site Scripting (XSS)		
Instructions			
Setup / Reset DB	AWAF can prevent ' or 1=1 #		
Brute Force	Message *		
Command Injection	Sign Guestbook Clear Guestbook		
CSRF			
File Inclusion			
File Upload	Name: test Message: This is a test comment.		
Insecure CAPTCHA			
SQL Injection	More Information		
SQL Injection (Blind)	<u>https://owasp.org/www-community/attacks/xss</u>		
Weak Session IDs	 <u>https://owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet</u> <u>https://en.wikipedia.org/wiki/Cross-site_scripting</u> 		
XSS (DOM)	<u>http://www.cgisecurity.com/xss-faq.html</u>		
XSS (Reflected)	• <u>http://www.scriptalert1.com/</u>		
XSS (Stored)			
CSP Bypass			
JavaScript			

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。



 Occurences をクリックし、誤検知したパラメータ名(mtxMessage)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=AWAF <mark>0x20can0x20prevent0x20or0x20</mark> 1=10x2 0#
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
Context	Documentation Documentation Parameter (detected in Form Data)
Parameter Level	Global
Actual Parameter Name	mtxMessage
Wildcard Parameter Name	*

AWAF v17.1 セットアップガイド

ONLINE (ACTIVE)						
Standalone						
Main Help About	Security » Options : Application Security : Attack Signatures : Attack Signatures List					
A Statistics	🚓 🗸 Attack Signatures 👻 Threat Campaigns RegExp Validator Integrated Services 👻 Advan			ferences		
_						
iApps					Create	Delete
S DNS	\[1 Entry
Local Traffic	Signature Name and Tag \wedge	Signature ID 🗘	Туре 🗘	Attack Type	Accuracy 🗘	Risk 🗘
Acceleration	SQL-INJ expressions like "OR 1=1" (7) (Parameter)	200002835	Request	SQL-Injection	MEDIUM	MEDIUM
Device Management	SQL-INJ expressions like "OR 1=1" (7) (Parameter)	\square				
📸 Shared Objects	Signature Type: Request	Summary: T	his event is gene	erated when an attempt is mad	e to exploit an SQL-Injection	
Con a surger	Signature Scope: Parameter/Cookie, XML, JSON, GWT, Plain Text	vulnerability	. This is a genera	al attack detection signature (i.e	e. it is not specific to any data	base or
Security	Attack Type: SQL-injection ⑦	web applicat	tion).			
Overview >	Systems: General Database	Impact: Suco	cessful exploitat	ion will result in information ga	thering and system integrity	o rocult
Guided Configuration	Accuracy: Medium	Possible exe	cution of arbitra	arv code of the attacker's choos	ing can result.	irresult.
Application Security	Last Updated: 2020-06-09	Detailed Info	ormation: SQL-I	njection occurs when a web ap	plication doesn't sanitize user	r-supplied
Protocol Security		input and pla	aces it directly in	nto the SQL statement. This eve	nt indicates that an attempt h	has been
Network Firewall		made by the	client to inject 9	5QL code into the application.		
DoS Protection		Affected Sys	stems: All system	ns with database connectivity a	re potentially affected.	application
Bot Defense		if user input	is not correctly	sanitized or checked before pas	ssing that input to the databa	application ise.
Event Logs		Ease Of Atta	ack: Vary from si	mple to medium.	0	
Reporting		False Positiv	ves: Some applic	ations send SQL statements to	the web server as legitimate	input.
Options >		Some free-te	ext user input m	ay match SQL-Injection signatu	res.	
		False Negati Corrective A	ives: None know	m. Ne system is using an up to date	version of the software and	has had all
Distributed Cloud Services		vendor supp	lied patches ap	plied.Utilize "Positive Security M	lodel" by accepting only know	vn types of
Retwork		input in web	application.			
		Additional R	teterences: http:	://www.webappsec.org/projects	s/threat/classes/sql_injection.	shtmi
system		See Less 🔺				

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

CONLINE (ACTIVE)				
Main Help About	Security » Application Security : Parameters : Parameters List			
Statistics	Parameters List Wildcards Order Extractions Character Sets	 Sensitive Parameters Navigation Para 	ameters	
iApps	🕏 DVWA_policy 👻 🔞 Learning Mo	de: Manual		Apply Policy
S DNS	Parameters List			
Local Traffic	Parameter Contains Go Show Filter Details	ε		Total Entries: 2
Acceleration		Legend: 🎧 V	Waiting for additional traffic samples 📿 Learning suggestions available 🥪 Rer	ady to be enforced Create
Device Management	A Parameter Name	Parameter Value Type	Parameter Level	Staging
-	•	Auto detect	Global	No
Shared Objects	UIEWSTATE	Ignore value	Global	No
Security	Change Type Enforce Delete Delete All			Total Entries: 2
Overview >				
Guided Configuration				
Application Security				
Dratacel Cacurity				

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。

ONLINE (ACTIVE) Standalone			
Main Help About	Security » Application Securit	ty : Parameters : Parameters List » Add Parameter	
Statistics	OVWA_policy	learning Mode: Manual	Apply Policy
iApps			Connect Connects
S DNS	Create New Parameter		Cancel Create
	Parameter Name	Explicit mb:Message	
E Local Traffic	Parameter Level	Global 🗸	
Acceleration	Location	Any	
	Perform Staging	Enabled	
Device Management	Is Mandatory Parameter	Enabled	
📸 Shared Objects	Allow Empty Value	Enabled	
~	Allow Repeated Occurrences	Enabled	
Security	Mask Value in Logs	Enabled	
Overview >	Parameter Value Type	Ignore value	
Guided Configuration	Cancel Create		
Application Security			

5. Apply Policy を押します。

Security » Application	Security » Application Security : Parameters : Parameters List						
🔅 👻 Parameters List	Wildcards Order	Extractions	Character Sets	Sensitive Parameters	Navigation Parameters		
DVWA_policy Control Contro Control Control Control Control Control Control Control Control Co				▲ Changes details (not applied) +	Apply Policy		
Parameters List							
Parameter Contains	 Image: Image: Ima	Go Sho	ow Filter Details >				Total Entries: 3

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。

÷	→ C A Not secure 1	0.1.10.180/DVWA/vulnerabilities/xss_s/
	VWA_VIP	
		DYWA
	Home	Vulnerability: Stored Cross Site Scripting (XSS)
	Instructions	
	Setup / Reset DB	
	Brute Force	Message *
	Command Injection	Sign Guestbook Clear Guestbook
	CSRF	
	File Inclusion	
	File Upload	Name: test Message: This is a test comment
	Insecure CAPTCHA	
	SQL Injection	Name: AWAF sales Message: AWAF can prevent ' or 1=1 #
	SQL Injection (Blind)	
	Weak Session IDs	More Information
	XSS (DOM)	https://owasp.org/www-community/attacks/xss
	XSS (Reflected)	<u>https://owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet</u> ttps://en.wikipedia.org/wiki/Cross-site_scripting
	XSS (Stored)	http://www.cgisecurity.com/xss-faq.html http://www.cgisecurity.com/xss-faq.html
	CSP Bypass	
	JavaScript	

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。

AWAF v17.1 セットアップガイド

CONLINE (ACTIVE) Standalone			
Main Help About	Security » Application Securit	v : Parameters : Parameters List -> Parameter Properties	
Statistics	🔅 🗸 Parameter Properties		
iApps	Edit Parameter		Cancel
	Parameter Name	mb:Message (Explicit)	
5 UNS	Parameter Level	Global	
Local Traffic	Location	Any	Cancel Ubdat
	Perform Staging	Enabled	
Acceleration	Is Mandatory Parameter	Enabled	
Device Management	Allow Empty Value	Enabled	
	Allow Repeated Occurrences	Enabled	
Shared Objects	Mask Value in Logs	Enabled	
Security	Parameter Value Type	User-input value	
Overview >	Data Type Value Meta Character	Attack Signatures	
Guided Configuration			
Application Security >	Check attack signatures and	Intreal campaigns on this parameter	alia: Callinas:
Protocol Security >	Attack Signature	tgs. State	olicy Settings.
Network Firewall	SQL-INJ expressions like "	OR 1=1" (7) (Parameter)	
DoS Protection			
Bot Defense >			
Event Logs >			
Reporting >			Ψ.
Options >		20002835	Total: 0
-	Cancel Update		

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。

← → C ▲ Not secure 10.	.1.10.180/DVWA/vulnerabilities/xss_s/	☆	Θ	:
DVWA_VIP				
	DYWA			
Home	Vulnerability: Stored Cross Site Scripting (XSS)		-	
Setup / Reset DB	Name *			
Brute Force Command Injection	Message *			
CSRF File Inclusion				
File Upload	Name: test Message: This is a test comment.			
Insecure CAPTCHA SQL Injection	Name: AWAF sales Message: AWAF can prevent ' or 1=1 #			
SQL Injection (Blind) Weak Session IDs	Name: AWAF sales Message: AWAF can prevent ' or 1=1 #			
XSS (DOM)	More Information			
XSS (Stored) CSP Bypass JavaScript	<u>https://owasp.org/www-community/attacks/xss</u> <u>https://owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet</u> <u>https://en.wikipedia.org/wiki/Cross-site_scripting</u> <u>http://www.cgisecurity.com/xss-faq.html</u> <u>http://www.scriptalert1.com/</u>			

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ことがあります。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。)

Alar	m 🗌 Blo	ck Violation	
	~	Threat Campaign detected -	

 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。

Security » Event Logs : Application : Requests		
🕁 🚽 Application 👻 Protocol 👻 Network	✓ DoS ✓ Bot Defense ✓ Logging	ng Profiles
□ Order by Date - Oldest ↑ 🗸 - Applied Filter: Illeg	gal Requests 🔀	C 🌣 - Total Entries: 11
Requests «	Delete Request Export Request	
☑ [HTTP] /path 5		
● 10.1.10.4 04:36:59 2019-02-20 N/A	▼ [HTTP] /path	
[HTTP] /index.php 5	✓ Triggered Violations	
 10.1.10.4 04:37:04 2019-02-20 N/A 	Violation	Occurrences Suggestions
[HTTP] /index.php 5	▼ Threat Campaign detected -	1 ▼ None
● 10.1.10.4 05:26:27 2019-02-20 N/A	✓ Request Details	Basic All Details
□[HTTP]/ 5	Geolocation - 🔻 🗑 N/A	Time 7 2019-02-20 04:36:59
05:26:34 2019-02-20 N/A	Source IP Address - 7 10.1.10.4:49844	Violation Rating 7 5 Request is most likely a threat
[HTTP] /path 5	Session ID - T 3fddde982130c67f	Attack Types N/A
 10.1.10.4 05:26:40 2019-02-20 N/A 	Microservice TV/A	
[HTTP] /path 5	✓ Request	
05:27:11 2019-02-20 N/A	Request actual size: 1435 bytes.	
[HTTP] /index.php 5	GET /path HTTP/1.1	
10.1.10.4 06:03:13 2019-03-22 N/A	Accept-Encoding: identity	
(HTTP) (index action 5	Content-Type: %{(#_='multipart/form-data').	.(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_membe
International data in the second s	<pre>rAccess?(#_memberAccess=#dm):((#container=#</pre>	<pre>#context['com.opensymphony.xwork2.ActionContext.contain</pre>
04:39:08 2019-07-15 N/A	<pre> er']).(#ognlUtil=#container.getInstance(@container.getInstance)</pre>	om.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUti

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。)

ONLINE (ACTIVE) Standalone Live Updates Available	Apply Policy Configuration Operation completed successfully.	
Main Help About	Security » Application Security - Policy Building - Learning and Ellocking Settings	
Mage Statistics	🔅 🚽 Traffic Learning Learning and Blocking Settings	
iApps	DVWA_policy V 🔅 🧇 Learning Mode: Manual	Apply Policy
Local Traffic	Policy Building Settings	Blocking Settings Search in Policy Building Settings
Acceleration	▶ Antivirus	
-	▼ Attack Signatures	
Device Management	Learn Alarm Block Signature Set Name	Signature Set Category
📸 Shared Objects	PHP Signatures (High/Medium Accuracy)	Change signature properties - User-defined
	MySQL Signatures (High/Medium Accuracy)	Change signature properties - User-defined
Security	Apache/NCSA HTTP Server Signatures (High/Medium Accuracy)	Change signature properties - User-defined
Overview	Generic Detection Signatures (High/Medium Accuracy)	Change signature properties - Basic
Guided Configuration		Change
Application Security	Auto-Added Signature Accuracy in Manning Arranges false in Hendrade semantice with num arranges in the international semantice with number international semantice wither in	
Protocol Security	Updated Signature Enforcement V Retain previous rule enforcement and place updated rule in staging	
Network Firewall	Attack Signature False Positive Mode Disabled	
DoS Protection	Note: If a signature false-positive is allowed this signature will not block the request.	
Bot Defense	Apply Response signatures for these File Types	
Cloud Services		
Event Logs		
Reporting		
Options	Delete	
	CSRF Protection	

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。

ONLINE (ACTIVE) Standalone Live Updates Available	
Main Help About	System » Software Management : Live Update
Mag Statistics	Image List Hotfix List Boot Locations Update Check
iApps	Install All Updates Upload File Last Check for Updates Details -
Local Traffic	

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。)

Updates Status	×
Checking for updates This may take several minutes. Please wait until the process is over	

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。を推し、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。

ONLINE (ACTIVE) Standalone Live Updates Available	_			
Main Help About	System » Software Management : Live Up	Jate		
Statistics	🚓 👻 Image List 👻 Hotfix List	- Boot Locations Updat	e Check Live Update	
iApps	Install All Updates Check for I	Jpdates Upload File	Last Check for Updates Details 👻	
Local Traffic				
Acceleration	Updates Configuration			Save
Device Management	ASM Attack Signatures	Installation of Automati	cally Disabled Real Tim	ne Scheduled
📸 Shared Objects				
Security	Bot Signatures	Installation Histo	У	
Network	Browser Challenges	Install Date	Update File Name	Status
System	Server Technologies		ASM-AttackSignatures_20201001_175533.in	n 😔 Pending (Preview Available)
Configuration		2020 08 24 16:05:45		
File Management	Threat Campaigns	2020-08-24 16:05:45	ASM-AttackSignatures_20190716_122131.in	n 🕑 Currentiy Installed
Certificate Management				
Disk Management				
Software Management				
License				

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 が完了すると以下のようになります。を推し、画面を閉じます。

Install Updates	×
ASM-AttackSignatures 20201001 175533 im	
,, (data)	
BotSignatures_20201001_174550.im	

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

System » Software Management : Live Updat	0				
🔅 🚽 Image List 👻 Hotfix List	✓ Boot Locations Upda	te Check Live Update			
Install All Updates Check for Upd	dates Upload File	Last Check for Updates I	Details 👻		
Updates Configuration					Save
ASM Attack Signatures	Installation of Automat Downloaded Updates	tically Disabled	Real Time	Scheduled	
Bot Signatures	Installation Histo	ory			
Browser Challenges	Install Date	Update File Name		Status	
Server Technologies	2020-10-04 21:05:05	ASM-AttackSignatures_2020	1001_175533.im	 Currently Installed 	
Threat Campaigns	2020-08-24 16:05:45	ASM-AttackSignatures_2019	0716_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 Result	S				
Added Entities (1513)				
Modified Entitie	s (1653)				
	Install Delete Cancel				

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。



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。

rity » Application Security : Security Po	licies : Policies List » DVWA_p	plicy		
curity Policy Configuration	✓ 0 Signatures ready to I	be enforc	ed 🕥 2 Sign	atures have si
General Settings	প-			
nheritance Settings	Basic Attack Signature Name		Adv	anced
licroservices	Attack Signature Name			
ttack Signatures	Status Staging			
hreat Campaigns	Signature ID Signature ID		User-Defined Yes	No
esponse and Blocking Pages	Signature Scope		Signature Type	-
	Any Scope	~	Request	Response
	Attack Type			
	Attack Type Name			
	Systems			
	Specify one or few syst	ems		

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。

Export -						Apply Policy
curity Policy Configuration	⊘ 0 Signatures ready to be enforced	tures have suggestions		Enforce ··	• Stage	e Disabl
eneral Settings	√			1 - 20	of 885 Entrie	s 1245
heritance Settings	Signature Name	Signature ID 🗘	Learn	Alarm	Block	Status
	System" injection attempt (Header)	200004200	 	~	~	Staging
icroservices	Isystem" injection attempt (Parameter	r) 200004199	 	×	~	Staging
tack Signatures	System" injection attempt (URI)	200004201	 Image: A second s	×	~	Staging
reat Campaigns	"vBulletin widgetConfig Render Code	200004995	~	~	~	Staging
ananaa and Dissking Dages	Script>alert(1); (Header)	200101610	×	~	~	Staging
sponse and blocking Pages	Script>alert(1); (Parameter)	200101609	~	~	~	Staging
	🗋 🕨 alert() (3) (Header)	200101624	~	~	~	Staging
	🗌 🚺 alert() (3) (Parameter)	200101623	~	~	~	Staging
	alert() (3) (URI)	200101625	~	~	~	Staging
	AngularJS Sandbox Escape - construct	. 200101352	~	~	~	Staging
	AngularJS Sandbox Escape - construct	 200101351	~	~	~	Staging
	AngularJS Sandbox Escape - construct	. 200101353	~	~	~	Staging
	Apache mod_proxy Connection DoS	200012065	~	~	~	Staging
	🗌 ▶ autofocus (Header)	200001582	~	~	~	Staging
	autofocus (Parameter)	200001581	~	~	~	Staging
	🗌 📘 autofocus (URI)	200001718	~	~	~	Staging
	Codelgniter RCE Gadget Chain	200104348	1	1	4	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 テスト前に行って下さい。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。

 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。

Main Help About	Security » Options : Application Security : Attack Signatures					ministration
Mage Statistics	Attack Signatures 👻 Threat Campaigns RegExp Validator	Integrated Services - Advanced Configuration	Synchronization	Preferences		
iApps					Create	Delete
S DNS	∀-			1 - 20 of	f 8071 Entries 1 2 3	4 404 🚺
Local Traffic	BASIC ADVANCED	Signa	ture ID 🗘 🛛 Type 🗘	Attack Type	Accuracy 🗘	Risk 🗘
Acceleration	References	20010	1559 Request	Cross Site Scripting (XSS)	MEDIUM	MEDIUM
Device Management	CVE + 2017-5638	20010	1558 Request	Cross Site Scripting (XSS)	MEDIUM	MEDIUM
Nhared Objects	Update Date	20010	0092 Request	Predictable Resource Location	MEDIUM	LOW
Security	Risk	20010	0093 Request	Predictable Resource Location	MEDIUM	LOW
Overview	LOW MEDIUM HIGH	20010	0094 Request	Predictable Resource Location	MEDIUM	LOW
Guided Configuration	Accuracy LOW MEDIUM HIGH	20010	0095 Request	Predictable Resource Location	MEDIUM	LOW
Protocol Security	Annly	20010	0108 Request	Predictable Resource Location	MEDIUM	LOW
Network Firewall	Sector and the second s	20010	0109 Request	Predictable Resource Location	MEDIUM	LOW
Bot Defense	"%CommonProgramW6432%" access (Header)	20001	0211 Request	Predictable Resource Location	MEDIUM	MEDIUM
Event Logs	"%CommonProgramW6432%" access (Parameter)	20001	0210 Request	Predictable Resource Location	MEDIUM	MEDIUM
Options	"%COMPUTERNAME%" access (parameter)	20010	0096 Request	Predictable Resource Location	MEDIUM	LOW

6	ONLINE (ACTIVE) Standalone						
Main	Help About	Security » Options : Application Security : Attack Signatures					
Statie	stics	🔅 🗸 Attack Signatures 👻 Threat Campaigns RegExp Validator Integrated Services 👻 Advanced Config	juration 👻 Synchronia	zation - Prefe	ences		
iApp:	s					Create	Delete
		V = CVE reference contains: 2017-5638					15 Entries
Loca	I Traffic	Signature Name and Tag \land	Signature ID 🗘	Туре 🗘	Attack Type	Accuracy 🗘	Risk 🗘
Acce	leration	Code Injection Java (Accessing attributes)	200004156	Request	Server Side Code Injection	MEDIUM	MEDIUM
Devic	ce Management	Code Injection Java (Accessing attributes) (#_classResolver)	200004262	Request	Server Side Code Injection	LOW	нібн
share	ed Objects	Code Injection Java (Accessing attributes) (#_keepLastEvaluation)	200004265	Request	Server Side Code Injection	LOW	нібн
Secu	rity	Code Injection Java (Accessing attributes) (#_lastEvaluation)	200004264	Request	Server Side Code Injection	LOW	нібн
0	verview	Code Injection Java (Accessing attributes) (#_traceEvaluations)	200004263	Request	Server Side Code Injection	LOW	HIGH
-	Guided Configuration	Code Injection Java (Accessing attributes) (#_typeResolver)	200004261	Request	Server Side Code Injection	LOW	нібн
	Protocol Security >	Java code injection - Content-Type class github.com/joaomatosf/jexboss	200004287	Request	Server Side Code Injection	HIGH	нібн
	Network Firewall	Java code injection - Content-Type class org.jboss.console.remote.RemoteMBeanInvocation	200004286	Request	Server Side Code Injection	HIGH	HIGH
	Bot Defense	Java code injection - jexboss webshell	200004288	Request	Server Side Code Injection	MEDIUM	нібн
Ev	rent Logs	Java code injection com.opensymphony (Header)	200003471	Request	Server Side Code Injection	HIGH	HIGH
Re	eporting >	Java code injection com.opensymphony (Parameter)	200003470	Request	Server Side Code Injection	HIGH	HIGH
C Distri	ibuted Cloud Cemises	Java code injection com.opensymphony (URI)	200003472	Request	Server Side Code Injection	нісн	нібн
O Note	iouteu ciouu services	JBOSS admin panel URL 3	200010106	Request	Predictable Resource Location	MEDIUM	MEDIUM
E Suete	am .	JSP Expression Language Expression Injection (URI)	200004281	Request	Server Side Code Injection	LOW	нідн
GT Syste		Object Graph Navigation Library Expression Injection (URI)	200004280	Request	Server Side Code Injection	LOW	нібн

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。

P Addresses and Geolocations					
Learn	Alarm	Block	Violation		
	Z	Z	Access from disallowed Geolocation -	7	
	~	~	Access from malicious IP address -	7	
	~	<	Bad Actor Detected -		
	Z	Z	IP is blacklisted -		

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

ONLINE (ACTIVE) Standalone						
Main Help About	Security » Application	Security : Security Policies : Policies Lis	t			
Statistics	🔅 🗸 Policies List	Policy Groups Policies Summary	Policy Diff			
iApps					Create	compare Delete
S DNS	∀-					1 Entry
Local Traffic	Policy Name ^	Enf	forcement Mode 🔇	Virtual Server(s)	Last Modified 🗘	OWASP Compliance
Acceleration	DVWA_policy	0	Blocking	DVWA_HTTPS_VIP	2023-08-25 16:57:28	1 / 10 =
Device Management						
Shared Objects						
Security						
Overview						
Guided Configuration						
Application Security >						

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。

Standalone			
Main Help About	Security » Application Security : Security Poli	cies : Policies List » DVWA_policy	
Statistics	Export • Enforce	ement Mode: 🦁 Blocking Learning M	Mode: Manual Apply Policy
S DNS	Policy Configuration		Save
Acceleration	General Settings	Trust XFF Header	Note: Response codes 200 through 399 are automatically allowed by the system Enabled Disobled
Device Management	Audit Log		
Shared Objects	Attack Signatures	Advanced Settings	
Security	Threat Campaigns	Server Technologies	MySQL X @ PHP X Apple Of CAUTO Energy X
Guided Configuration	IP Intelligence	Policy is Case Sensitive	Yes
Protocol Security	IP Address Exceptions	Geolocation Enforcement	Disallow Access Allow Access
DoS Protection	Sessions and Logins		Afghanistan
Bot Defense > Event Logs	Response and Blocking Pages		Albania
Reporting >			American Samoa
Options	HTTP Message Protection	Differentiate between HTTP/WS and HTTPS/WSS URLs	Enabled Disabled

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。Appliction 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。

Standalone					
Main Help About	Security » Application Security : Security Policie	s : Policies List			
Mage Statistics	Policies List Policy Groups Polic	ies Summary Policy Diff			
iApps				Create	••• Compare Delete
S DNS	₹.				1 Entry
Local Traffic	Policy Name	Enforcement Mode 🗘	Virtual Server(s)	Last Modified 🗘	OWASP Compliance
Acceleration		Slocking	DVWA_HTTPS_VIP	2023-08-25 16:57:28	1 / 10 =
Device Management					
shared Objects					
Security					
Overview					
Guided Configuration					
Application Security >					

2. **IP Intelligenc** を On にします。

Standalone			
Main Help About	Security » Application Security : Security F	volicies : Policies List » DVWA_policy	
Statistics	Export • Ent	orcement Mode: 🦁 Blocking 📔 Learning Mode: Manual	Apply Policy
iApps			
S DNS	Policy Configuration		Save
Local Traffic	,		
Acceleration	General Settings	IP Intelligence ⑦ Last Update: 2023-08-25 18:06:13 -	OFF
Device Management	Audit Log		
Shared Objects	Attack Signatures		
Security	Threat Campaigns		
Overview	Threat Campaigns		
Guided Configuration	IP Intelligence		
Application Security >			

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。
| ONLINE (ACTIVE)
Standalone | | | | | | | |
|-------------------------------|--|---|---------------------------|-------|---------------------|----------|---------------------|
| Main Help About | Security » Application Security : Security I | Policies : Policies List » DVWA_policy | | | | | |
| Statistics | ← Export ▼ En | nforcement Mode: 🥏 Blocking 🕴 Learning Mc | de: Manual | | | Ap | oly Policy |
| iApps | | • • • • | | | | | |
| S DNS | | 1 | | | | / | |
| Local Traffic | Policy Configuration | | | | | | Save |
| Acceleration | General Settings | IP Intelligence ⑦ Last Up | date: 2023-08-25 18:06:13 | 3 - | | | ON |
| | A | | | | | | _ |
| Device Management | Audit Log | | Alarm | Block | | Alarm | Block |
| Shared Objects | Attack Signatures | Tor Proxies 🔞 | | | Denial of Service 🔞 | | |
| Security | Threat Compaigns | Mobile Threats ③ | | | Scanners 💿 | | |
| Overview | , intreat Campaigns | Cloud-based Services (2) | | | BotNets (?) | | |
| Guided Configuration | IP Intelligence | | | | | | |
| Application Security | | Anonymous Proxy ⑦ | | | Web Attacks ⑦ | | |
| Protocol Security | IP Address Exceptions | Phishing Proxies (2) | | | Windows Exploits ③ | ~ | |
| Network Firewall | | - | _ | _ | | _ | - |
| DoS Protection | Sessions and Logins | Infected Sources (2) | | | Spam Sources 🕜 | | |
| | | | | | | | |
| Bot Defense | | | | | | | $ \longrightarrow $ |

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。

ONLINE (ACTIVE) Standalone				
Main Help About	Security » Application Security : Security Poli	icies : Policies List » DVWA_policy		
Statistics	Export • Enfor	cement Mode: 🥏 Blocking Lean	ning Mode: Manual	Apply Policy
iApps				
S DNS	Policy Configuration			Save
Acceleration	General Settings	Blocking Page Default	Response Type Default Response 🗸	
Device Management	Audit Log		Response Headers Response Body [] HTTP/1.1 200 OK	
Shared Objects	Attack Signatures		Cache-Control: no-cache Pragma: no-cache Connection: Close	
Security	Threat Campaigns	Loria Dere		
Overview		Login Fage	Response Type Default Response 🗸	
Guided Configuration	IP Intelligence		Response Headers Response Body	
Protocol Security	IP Address Exceptions		НТТР/1.1 200 ОК	
Network Firewall			Pragma: no-cache	
DoS Protection >	Sessions and Logins		Connection: close	
Bot Defense >		XML	Personana Tuna COAD Faula	
Event Logs >	Response and Blocking Pages		Response Type SOAP Fault	
Reporting			Response Headers Response Body	
Options >	HTTP Message Protection		НТТР/1.1 200 ОК	
Distributed Cloud Services	Advanced Protection		Pragma: no-cache Content-type: text/xml Contention: clore	

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

Security » Application Security : Security Police	cies : Policies List » DVWA_policy		
Export • Enforce	ement Mode: 🥏 Blocking Lean	ning Mode: Manual	Apply Policy
Policy Configuration			Save
General Settings	Blocking Page Default	Response Type Custom Response 🗸	
Audit Log		Response Hea Custom Response HTTP/1.1 200 G Redirect URL control Response	
Attack Signatures		Cache-Control: Erase Cookies Pragma: no-cache Conpertion: Cope	
Threat Campaigns		Restore Default Headers	
IP Intelligence	Login Page	Response Type Default Response	
IP Address Exceptions		Response Headers Response Body []	
Sessions and Logins		Cache-Control: no-cache Pragma: no-cache Connection: close	
Response and Blocking Pages	XML	Response Type SOAP Fault	

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

Security » Application Security : Security Polici	es : Policies List » DVWA_policy		
Export • Enforce	ment Mode: 🥏 Blocking 📋 Learn	ing Mode: Manual	Apply Policy
Policy Configuration			Save
General Settings	Blocking Page Default	Response Type Custom Response 🗸	Â
Audit Log		Response Headers Response Body []	
Attack Signatures		<html><head><title>アクセス科師可</title></head><body>あなたはこちらのサイトへ 理想までご理解ください。 くなっなかる問い合わせ振号はこちらです。:<htps: td="" www.secondecondecondecondecondecondecondecond<=""><td>のアクセス許可されておりません。F5管 ()%><b;>><b;>><a< td=""></a<></b;></b;></td></htps:></body></html>	のアクセス許可されておりません。F5管 ()%> <b;>><b;>><a< td=""></a<></b;></b;>
Threat Campaigns		Restore Default Body Upload File	
IP Intelligence	Login Page	Response Type Default Response	
IP Address Exceptions		HTTP/1.1 200 OK	
Sessions and Logins		Cache-Control: no-cache Pragma: no-cache Connection: close	
Response and Blocking Pages	XML	Response Type SOAP Fault	

4. 右上の枠のようなボタンを押します。

Export • Enfo	rcement Mode: 🥏 Blocking Learr	ing Mode: Manual	Apply Policy
Policy Configuration			Save
General Settings	Blocking Page Default	Response Type Custom Response	A
Audit Log		Response Headers Response Body [] cbody>あなたはごちらのサイトへのアクセス許可されて ・	
Attack Signatures		おりません。FS電球者までご注照くたさい。 <pre>cpr>cpr>b 問い合わせ番号はこちらです。</pre> - kpr>chr	
Threat Campaigns		Restore Default Body Upload File	
IP Intelligence	Login Page	Response Type Default Response 🗸	
IP Address Exceptions		Response Headers Response Body []	
Sessions and Logins		Cache-Control: no-cache Pragma: no-cache Cappertion: dore	
Response and Blocking Pages	XML	Response Type SOAP Fault	

5. ブロックページのレビューが表示されます。

General Settings	Blocking Page Default	Response Type Custom Response	•
		Response Headers Response Body	2
Audit Log		<body>あなたはこちらのサイトへのアクセス許可されて</body>	
Attack Signatures		おりません。FS官任者までご理解くたさい。 bp > bp > bp > bp > bp > bp > bp >	
Threat Campaigns	Response Body P	Preview ×	
P Intelligence	あなたはこちらのサイトへの	アクセス許可されておりません。F5管	
P Address Exceptions	理者までご理解ください。	E :	<u> </u>
	お問い合わせ番号はこちらで	す。: <%TS.request.ID()%>	
Sessions and Logins			

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。

Security » Application Security : Security Polic	ies : Policies List » DVWA_policy			
Export - Enforce	ement Mode: 🥑 Blocking Learni	ing Mode: Manual	⚠ Changes details (not applied) →	Apply Policy
Policy Configuration				Save
General Settings	Blocking Page Default	Response Type Custom Response	~	î
Audit Log		Response Headers Response Body	£3	
Attack Signatures		<body>あなたはこちらのサイトへのアクセス許可されておりません。F5管理者までご理解ください。 くたっくby>お問い合わせ番号はこちらです。:<%TS.request.D0%></body>	•	
Threat Campaigns		Restore Default Body Upload File		
IP Intelligence	Login Page	Response Type Default Response	~	
IP Address Exceptions		Response Headers Response Body	£3	
Sessions and Logins		Cache-Control: no-cache Pragma: no-cache Connection: close		
Response and Blocking Pages	XML	Response Type SOAP Fault	•	

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!