## **MONITOR PP**



.

# Table of Contents

Overview for AIWAF-VE menu	3
Configuration of AIWAF-VE	4
1. Subscribe AIWAF-VE BYOL or PAYG:	4
2. Access the Web User Interface (UI):	4
3. Register Your License(AIWAF-VE BYOL only ):	6
4. Time Zone and Language Setting:	7
5. Update Signature and Geolocation DB:	8
6. Register Protected Web Servers:	9
6-1. Register HTTP Web Servers	9
6-2. Register HTTPS Web Servers	12
6-3. Apply Policy	16
6-4. Security Policy Block Mode Configuration	17
7. Complete Configuration:	20
Testing AIWAF-VE: Procedure for Test	21
Step 1: Redirect Test Traffic to AIWAF-VE:	21
Step 2: Send Sample Traffic to AIWAF-VE:	21
Step 3: Verify Attack Detection:	22
Contact us	23

## Overview of AIWAF-VE menu

Menu	Description
Monitoring	Provides a centralized visual representation of web traffic, system information, detection counts, detection severity, and the detection log of your web server. It is a user interface that allows users to monitor and analyze real-time or historical data in a concise and easily understandable format.
Log analysis	Provides a platform for analyzing and interpreting detection log, audit log, and web server status log data. This menu is designed to assist users in gaining insights from large volumes of log entries, uncovering meaningful patterns, trends, anomalies, and security-related information.
Report	Generating, viewing, and managing various types of reports (detection log, web traffic, web accelerator, system, and policy settings) that summarize and present information from the registered domain. This menu provides a concise and organized overview of data, metrics, trends, and analysis results.
Policy settings	Configuring and managing the protected web server along with the security policies that govern the behavior of the AIWAF-VE. This menu empowers administrators to configure and fine-tune security policies, determining how the AIWAF-VE detects, prevents, and responds to potential threats targeting web servers.
Configurations	Offers various configurations for AIWAF-VE, including administrator, system, NIC, product settings, log management, and service control.

## Configuration of AIWAF-VE

## 1. Deploy the AIWAF-VE Image:

- Upload the downloaded AIWAF-VE image file (ova, vhd, vmdk) to your preferred environment and boot it up.
- Subscribe to the AIWAF-VE and allocate an instance according to the procedures of your CSP.

## 2. Access the Web User Interface (UI):

Sign In Please enter your admin account.
administrator
English
Sign In

Open your internet browser and access the GUI by entering the assigned IP for the instance as follows: https://[AIWAF-VE IP]:222.
 (a.g., if your assigned IP for the instance is 102 169 10 110, the UPL is https://102 169 10 110:222)

(e.g., if your assigned IP for the instance is 192.168.10.110, the URL is <u>https://192.168.10.110:222</u>)

- Please change the language before sign in. (Supported languages: English, Japanese, Korean
- Login with the provided ID and Password (ID: administrator, PW : \_appleader)

#### APPLICATION INSIGHT WAF

Monitoring	Log ana	ilysis	Report	Policy settings	Configurations
Dashboard					
You are using	the default ID and	the default passw	ord. Please change	ID and password	rd.
• Administrato	r settings				0
Name		Administrator			
ID		administrator			
Password		Current passwo	rd		
		New password			
		Confirm new pa	ssword		
Password ch	nange notification	60 day(s)			
Two-Factor A	Authentication	Use	Not use		
Allowed IP		IP		+ 🖶	
Recipient E-	mail	E-mail		+ 🖶	
Explanation					
Capitalian					1
Apply					

#### 

- After your first login, please change the **default ID** and **Password** and specify **Allowed access IPs** for the security.
- Password change menu location : Configurations → Administrator settings → click 'Change' button.

APPLICATION INSIGHT WAF

## Oconfigure Static IP (Optional):

APPLICATION IN	SIGHT WAF							
Monitoring	Log analysis	Report	Policy settings	Configurations				
Administrator settings	s System setting:	s NIC settings	Product settings	Log management	Service control			
Click menu title to move t	« to the menu	습 IP settings						0
<ul> <li>IP settings</li> </ul>		Туре	ODHCP	STATIC				
<ul> <li>Mail settings</li> </ul>		IP	IP Version	IPv4 O IPv6				
• Telegram notification se	ttings			✓ IP	Netmask	Gateway	+ 😚	
• Backup server settings								
<ul> <li>Hostname settings</li> </ul>								
• Time synchronization se	ettings							
<ul> <li>Time zone settings</li> </ul>								
<ul> <li>SNMP GET settings</li> </ul>		mgmuie						
<ul> <li>SNMP TRAP settings</li> </ul>		Netmask						
		Gateway						
		DNS 1						
		DNS 2						
							Арр	ly

If you are using a static IP, follow these steps: Go to Configurations → System settings → IP settings. Select 'STATIC,' enter the IP settings and gateway value, click +, and then click 'Apply' to complete the process.

## 3. Register Your License (for BYOL only):

\*If you are a PAYG (Pay-As-You-Go) user, you can skip the license installation step since your plan already includes the necessary license.

Monitoring	Log analysis	Report	Policy settings	Configurations			
Administrator settings	System settin	igs NIC settings	Product settings L	₋og management	Service control		
	«						Apply
Click menu title to move t	to the menu						
		Online update L	icense update				
<ul> <li>Language settings</li> </ul>							
<ul> <li>License management</li> </ul>		Use/Not use	Use	◯ Not use	\$		
• HA settings		Activation Code	8characters	- 4charac - 4chara	- 4charac - 12character	S Check	
<ul> <li>Configurations synchron</li> </ul>	nization	Server address	O IP:				
setungs			Domain:		P	Port: 443 ≯	
<ul> <li>Program/Configuration b</li> </ul>	backup		L L				
<ul> <li>National IP DB settings</li> </ul>							Apply
<ul> <li>Whois settings</li> </ul>							
<ul> <li>Open API settings</li> </ul>							
		☆ HA settings					0
		HA mode	Not use	◯ Active-	Standby		
							Apply
							Арріу

- Access: Configurations → Product settings → License management → Online update.
- Choose your online update preference (enable/disable).
- Enter the Activation Code and click 'Check' to validate.
- Click 'Apply' to complete license registration.

## 4. Time Zone and Language Settings:

#### APPLICATION INSIGHT WAF

Monitoring	Log analysis	Report	Policy settings	Configurations	
Dashboard					
Click menu title to mo	ve to the menu	☆ Time zone setting	gs		0
• IP settings		Current time	Tue Aug 22 8:45:	14 KST 2023	
<ul> <li>Mail settings</li> </ul>		Time zone	Asia/Seoul	~	
• Telegram notification	n settings				Apply
<ul> <li>Backup server settin</li> </ul>	gs				, 46A
<ul> <li>Hostname settings</li> </ul>					
• Time synchronization	n settings	☆ SNMP GET settin	gs		0
• Time zone settings					
<ul> <li>SNMP GET settings</li> </ul>		SNMP MIBS list			
<ul> <li>SNMP TRAP setting</li> </ul>	s	Version	SNMPv2	○ SNMPv3	3
		o			

• Time zone Setup: Configurations > System Settings > Time zone Settings

#### APPLICATION INSIGHT WAF

Monitoring	Log analysis	Report	Policy settings	Configurations	
Administrator settings	System setting	s NIC settings	Product settings Lo	og management	Service control
	«				
Click menu title to move to	o the menu	☆ Language setting	5		0
e Language settings					
• Linner		Language	English	~	
<ul> <li>License management</li> </ul>					
<ul> <li>HA settings</li> </ul>					Apply
<ul> <li>Configurations synchroni settings</li> </ul>	ization				
• Program/Configuration b	ackup	☆ License managem	ient		٢
<ul> <li>National IP DB settings</li> </ul>		Product license			

Language Setup: Configurations > System Settings > Language Settings

## 5. Update Signature and Geolocation DB:

• You need to update the pattern signatures and geolocation database.

APPLICATION I	NSIGHT WAF										
Monitoring	Log analysis	Report	Policy se	ettings	Configurations						
Default settings	Admin policy	Domain policy	Policy test								
	×	☆ Pattern upda	te settings								
Click menu title to more	ve to the menu	Pattern update	server								0
<ul> <li>Operation mode</li> </ul>		Server address	(	O IP:							
• User authentication			(	Domain:	api.monitorapp.com		Port:	443	*		
<ul> <li>System overload aut</li> </ul>	o bypass setting	Auto pattern upd	ate (	●Use Ot	Not use						
<ul> <li>Log abridgement</li> </ul>											
<ul> <li>Pattern detection mo</li> </ul>	de										Афріу
<ul> <li>Path case sensitive</li> </ul>		Online pattern	update								(?)
<ul> <li>Health check for prot servers</li> </ul>	lected web	The current patte	rn version V	V.5.0.057.000	07_20230727_79f5fc5e30c6	bc9be5a827dcd1	69051ccd	e6422c6052	0270ebd77112	89f425e1	
• Web server encoding	g settings	Latest pattern ve	rsion	Check versi	on W.5.0.057.0007_20230	727_79f5fc5e30c	6bc9be5a8	827dcd1690	51ccde6422c6	0520270ebd7711289	#425e1
<ul> <li>Multiple decoding de</li> </ul>	tect setting										Pattern undate
• Web shell solution in	terwork settings	1									
• Threat Intelligence(A	ICC) interwork	Offline pattern	update								(3)
setting		Upload pattern fil	le	Choose File	No file chosen						
<ul> <li>Passive mirror</li> </ul>											
<ul> <li>Passive Mirror VXLA</li> </ul>	N										Apply
<ul> <li>All policies response</li> </ul>	data logging										
<ul> <li>Custom page setup</li> </ul>		Auto Scalino	mode settings								0
<ul> <li>Pattern update settin</li> </ul>	gs	A Fato scaling	more setting:	•							•

- [Signature Update] To access, go to: Policy settings → Default settings → Pattern update settings → Online pattern update.
- If the checkbox displays 'The current pattern version is the latest version' it indicates that the latest pattern is applied.

APPLICATION INS	SIGHT WAF				
Monitoring	Log analysis	Report Pa	licy settings	Configurations	
Administrator settings	System settings	NIC settings Pro	duct settings Lo	og management	Service control
Click menu title to move to	o the menu	3			
<ul> <li>Language settings</li> </ul>	合	lational IP DB setting	5		
License management	N	ational IP DB automatic	updates		0
<ul> <li>Configurations synchron settings</li> </ul>	ization Au	omatic update	<ul> <li>Use</li> </ul>	◯ Not us	8
• Program/Configuration b	ackup				Apply
National IP DB settings	N	ational IP DB file upload	i		0
<ul> <li>Whois settings</li> </ul>	Th	e current national IP DB i	nformation: GeoIP2 0	Country database, Bu	ild Epoch: 2019-12-24
<ul> <li>Open API settings</li> </ul>	File	upload	Choose File	No file chosen	
					Apply
	<b>公</b> 1	Vhois settings			٥

- [Geolocation Update] To update geolocation information, follow these steps: Go to Configurations → Product settings → National IP DB settings. Enable automatic updates 'Use' and click 'Apply.'
- Once you see the 'Completed' message, you can proceed to the next step.

## 6. Register Protected Web Servers:

HTTP and HTTPS (page #11) have separate registration procedures for protected websites.
 Follow the relevant procedure based on the website's protocol.

## 6-1. Register HTTP Web Servers

APPLICATION INSIGHT W	ΆF							
Monitoring Log analys	is Report	Policy settings	Configurations					
Default settings Admin policy	Domain policy Policy	y test						
Admin policy	Admin policy > Protecte	ed web server 🟠 Add	shortcut menu					
Protected web server Additional settings								Cert. Quick change Add rule
IP policy	- Use/Not use	All	∽ - Name		Certificate status	All 🗸	- Issued to	
IP Whitelist	- Protocol	All	<ul> <li>✓</li> <li>IP</li> </ul>		- Port		Host name	
IP Blacklist	<ul> <li>RX interface</li> </ul>	All	<ul> <li>TX interface</li> </ul>	All	<ul> <li>Explanation</li> </ul>			
DoS policy					_			
Session attack detection	U D				Q Search			15 line(s) 🗸
Slow DoS attack detection	∎ رڻ Na	ame 🔻 🛛 Pro	tocol 🔻 RX/TX 🔻		Web se	rver information		Explanation Change
Slow Read attack detection								
Priority policy					There is no data.			
URL access rule								

- To access, go to Policy settings → Admin policy → Protected web server, then click 'Add rule'.
  - $\checkmark\,$  No need for changes as HTTP is set as the default configuration.

Web server	
• Web server	
Use/Not use	Use ONot use
Name	CustomeName
Protocol	● HTTP ○ HTTPS
RX interface	eth0: 10.0.11.230 V Port 80
TX interface	eth0: 10.0.11.230 🗸
Receive Allowed IPs other than RX interface IP list	IP:PORT : + @
Web server information	Register new web server
Explanation	
Apply	

• Enter a custom name for the web server registration and then click 'Register new web server'.

id Web server		
URL http:// www.yourdomair	n.com / All(*)	
IP 192.168.0.100	Port 80 + 🖶	
Server Load Balancing Has	h 🗸	
SEL Termination	HTTPS Service port	

- Put your protected URL, IP address and Port number and click '+
- For servers with dynamic IP, use Lookup option for alias registration.

d Web server			
IRI http://www.vourdomai			
IP	Port	+ 🖶	
Server Load Balancing Ha	sh 🗸		
IP: 192.168.0.100	Port: 80		
□ IP: 192.168.0.101	Port: 80		
SSL Termination	HTTPS Service port		
			Add

• Once you have confirmed that the entered value is applied correctly, click 'Add' to continue.

	<ul> <li>Web server</li> </ul>		
	Use/Not use	● Use O Not use	
2	Name	CustomeName	
	Protocol	● HTTP ○ HTTPS	
J.	RX interface	eth0: 10.0.11.230 V Port 80	
	TX interface	eth0: 10.0.11.230 🗸	
	Receive Allowed IPs other than RX interface IP list	IP:PORT: + 世	
	Web server information	Register new web server           www.yourdomain.com         192.168.0.100:80, 192.168.0.101:80	
	Explanation		

• After verifying the entered web server information, click '**APPLY**' to finalize the web server registration.

Admin p	olicy > Protected wel	b server	☆ Add shortcut m	enu						
🕸 Suci	cessfully applied the p	oolicies. Do	o you want to app	bly the policies? To the Policies	cy management menu	pply policy Restored to the p	previous policies.		Cert. Quick change	Add rule
- Use - Prot - RX i	/Not use ocol nterface	All All All	× ×	- Name - IP - TX interface	All v	Certificate status     Port     Explanation	All	<ul> <li>Issued to</li> <li>Host name</li> </ul>		
	ტ					Q Search			1	15 line(s) 🗸
<b>•</b> 4	) Name 🔻	7	Protocol 🔻	RX/TX 🔻		Web serv	rer information		Explanation	Change
<u>ط</u>	CustomeName		HTTP	RX: eth0 10.0.11.230:80 TX: eth0 10.0.11.230	Host name: www.yourd - 192.168.0.100:80 - 192.168.0.101:80	Jomain.com				ľ
Total co	ount(s): 1 Case(s)					1				

• In the 'Protected web server' menu, you can see the registered web server.

#### 6-2. Register HTTPS Web Servers

#### APPLICATION INSIGHT WAF

Мо	nitoring Log a	analysis	Report	Policy settings	Config	urations								
De	fault settings Admin	policy	Domain policy Po	licy test										
¢ A	dmin policy		Admin policy > Prote	cted web server	습 Add shortcut menu									
	Protected web server													
	Additional settings												Cert. Quick change	Add rule
	IP policy		- Use/Not use	All	~	Name			- Certificate status	All	~	<ul> <li>Issued to</li> </ul>		
	IP Whitelist		- Protocol	All	~	IP			- Port			- Host name		
	IP Blacklist		- RX interface	All	× ·	TX interface	All	~	- Explanation					
	DoS policy													
	Session attack detection	in	<u>ြာ</u> ပြ					1	Q Search					15 line(s) 🗸
	Slow DoS attack detection	tion	∎ @	Name 🔻	Protocol	RX/TX 🔻			Web serv	er information			Explanation	Change
	Slow Read attack detec	ction												
	Priority policy							There	is no data.					
	URL access rule													

• Access: Policy settings → Admin policy → Protected web server → Click 'Add rule'

Web server	
• Web server	
Use/Not use	● Use O Not use
Name	CustomeNameHTTPS
Protocol	OHTTP INTPS
RX interface	eth0: 10.0.11.230 V Port 443
TX interface	eth0: 10.0.11.230 🗸
Receive Allowed IPs other than RX interface IP list	IP:PORT + 1
Web server information	Register new web server
Explanation	
Apply	

• Enter a custom name, ensure 'HTTPS' is checked, and then click 'Register new web server'.

d web server		
**If you do not use SSL offload, you	ı do not distinguish w	hether a URL has a path.
JRL https:// www.yourdomain2.com	/ All(*)	Lookup
P 192.168.0.100	Port 443 +	<b>e</b>
Server Load Balancing Hash	~	
HTTP Service port	Replace response	data
Select the other protected web server Not Use	✓ Web	server Not Use
Certificate file Choose File No	o file chosen	Automatic register Certificate file format (pfx)
Private key file Choose File No	o file chosen	Certificate verify
	-	
SL Connection priority OClient	Server	
SSL Connection priority OClient Extension function	Server Server HTTP/2 Suppo	rt
SSL Connection priority ○ Client Extension function ☑ Verify Not-allowed SSL Version ○ SSL	Server Server HTTP/2 Suppo . handshake denied	rt ● Block page The default block page ✔ Create log

- Put your protected URL, IP address and Port number and click '+
- For servers with dynamic IP, use Lookup option for alias registration.

Add Web server				×
**If you do not use SSL offload, you o	do not distinguish	whether a URL ha	s a path.	*
URL https:// www.yourdomain2.com	/ All(*)	Loo	kup	
IP	Port -	+ 🖶		
Server Load Balancing Hash	~			
IP: 192.168.0.100         Port           IP: 192.168.0.101         Port	: 443 : 443			
HTTP Service port Select the other protected web serverNot Use	Replace response	e data eb server <u>Not Us</u>	- <b></b>	
Certificate file Choose File No Private key file Choose File No	file chosen file chosen	Certificate	egister Certificate fil verify	e format (pfx)
SSL Connection priority OClient	Server			
Extension function	erver HTTP/2 Supp	oort		
Not-allowed SSL Version OSSL I	nandshake denied	Block page	The default block page $\checkmark$	Create log
	<b>a</b>			Add Close

- Verify the registered IP address and port number.
- Register the 'Certificate file', 'Private key file' and click 'Certificate verify' to proceed.

elect the other		
rotected web server Not Use V	eb server Not Use	
Certificate file Choose File monitorapp23_server.	crt Automatic register Certificate file format (pf)	x)
*.monitorapp.com	Certificate verify	
SL Connection priority OClient OServer		
	port	
ot-allowed SSL Version 🛛 🔿 SSL handshake denied	● Block page The default block page 🖌 🗌 Create	log
ncryption algorithm preference settings Olient	O Server(AIWAF)	
lient SSL Automatic selection of versions and algorith	Isme	
lient SSL version Minimum Allowable Protocol	TLSv1.0   Maximum Allowable Protocol	
lient Encryption algorithms		
□ == All Select ==	== All Select ==	
CDHE-RSA-AES256-SHA		
DHE-KSA-AE3250-SHA		
DHE-RSA-CAMELLIA256-SHA Dela		

- Once you've confirmed the certificate file and private key, proceed with the detailed configuration of the web server, including SSL/TLS versions and cipher suites, if necessary.
- Additionally, for [Client SSL Automatic selection of versions and algorithms], input the domain and IP to scan the cipher suite of the web server you are registering.

dd Web server
protected web server Not Use 🗸 Web server Not Use
Certificate file       Choose File       No file chosen       Automatic register       Certificate file format (pfx)         Private key file       Ctr Q.Automatic selection of versions and algorithms       Image: Xing Xing Xing Xing Xing Xing Xing Xing
SSL Connection priority Cipherscan
Extension function     Please enter server information.       Not-allowed SSL Versio     Please enter server information.       Please enter both IP and domain information for accurate scan     ge <ul> <li>Create log</li> <li>Create log</li> </ul>
[Client SSL Automatic s IP https:// 8.8.8.8
Client SSL version Domain https://www.google.com : 443 e Protocol
Client Encryption algor
== All Select ==
L ECDHE-RSA-AES25
DHE-RSA-CAMELLIA256-SHA Deide

- Enter the IP and domain information. The web server scanning will automatically select the SSL version and algorithms for the web server.
- After completing the previous steps,, click 'Add' to register web server information.

0	Web server		
	• Web server		
	Use/Not use	Use O Not use	
	Name	CustomeNameHTTPS	
	Protocol	OHTTP OHTTPS	
	RX interface	eth0: 10.0.11.230 V Port 443	
	TX interface	eth0: 10.0.11.230 🗸	
	Receive Allowed IPs other than RX interface IP list	IP.PORT : + *	
	Web server information	Register new web server           www.yourdomain2.com         192.168.0.100:443, 192.168.0.101:443	Delete
	Explanation		
	Apply		

• Once you've reviewed the provided information, click '**Apply**' to complete the process.

### 6-3. Apply Policy

APPLICATION	INSIGHT	WAF
-------------	---------	-----

Monitoring Log analysis		Rep	ort	Policy settings N	Configuration	s		
De	fault settings	Admin policy 🛚	Domain po	olicy Pol	icy test			
<b>‡</b> A	dmin policy N		🌣 Admin p	oolicy 값 A	dd shortcut menu			
	Protected web s	erver N					8	
	Additional sett	ings	Policy a	appiy/cance	1		3	
	IP policy				Policy		Changed items	
	IP Whitelist		Pro	tected web s	erver		1 Case(s) Q	
	IP Blacklist			Whitelist			0 Case(s)	
				Blacklist			0 Case(s)	
	Sossian attack	dataction	Session attack detection				0 Case(s)	
	Session attack detection			w DoS attack	0 Case(s)			
	Slow DoS atta	ck detection	Slow Read attack detection				0 Case(s)	
	Slow Read att	ack detection	URL access rule				0 Case(s)	
	Priority policy		Nat	ional IP deteo	ction		0 Case(s)	
	URL access ru	le	🗌 Use	er Manageme	nt		0 Case(s)	
	National IP de	tection	🗌 Use	er-defined rule	9		0 Case(s)	
	User-defined r	ule	Blo	ck page man	age		0 Case(s)	
	Block page ma	anage	Def	ault SSL			0 Case(s)	
	JRL Rewriting p	oolicy	🗌 Hea	alth-check UF	RL		0 Case(s)	
	URL Rewriting	request rule		L Rewriting re	equest rule		0 Case(s)	
	URI Rewriting	response rule		L Rewriting re	esponse rule		0 Case(s)	
_		policios		L Encryption	policies		0 Case(s)	
_		policies	🗆 API	policies			0 Case(s)	
	test		Apply	policy Re	estored to the previous	s policies.		
	hoiiang		Restore	policy			0	

- After registering the web server, configuring its details, and making changes to various
  policies, remember to click 'Apply policy ' in the Admin policy section of the upper-level menu
  to implement the changes. Otherwise, the changes will not be applied. (Previous policies will
  be backed up.)
- To access: Policy settings → Admin policy → Policy apply/cancel → click 'Apply policy'.

#### 6-4. Security Policy Block Mode Configuration

#### APPLICATION INSIGHT WAF

Monitoring	Log analysis	Report	Policy settings	Configurations
Default settings	Admin policy	Domain policy P	Policy test	
	×	☆ Operation mode	,	
Click menu title to move	e to the menu			
• Operation mode		Operation mode	O Policy b	bypass O Detection mode
<ul> <li>User authentication</li> </ul>		Bypass target	Request	Header name: Value     All headers are applied if there are no     +
o System overload auto	bypass setting		C [Reque	jest/Response] Content-Type:application/vnd.ms.wms-hdr.asfv1
<ul> <li>Log abridgement</li> </ul>				Jest/Response] Content-Type:application/x-mms-framed
• Pattern detection mod	e			uest/Response] Content-Type:application/x-wms-getcontentinto uest/Response] Content-Type:application/x-wms-LogStats
o Path case sensitive			L. coduo	1 3 Merekani
<ul> <li>Health check for prote servers</li> </ul>	cted web		URL Path	HTTP V :// 80 / ? + @
• Web server encoding	settings			
• Base64 decoding dete	ect setting			
• Multiple decoding dete	ect setting			
• Web shell solution inte	erwork settings		LIRI extens	nsion L 🖨
<ul> <li>Threat Intelligence(AIC setting</li> </ul>	CC) interwork			
Passive mirror				
• Passive Mirror VXLAN				
• All policies response d	lata logging			
• Custom page setup		Detection mode targe	ets URL HTT	TTP ♥ :// : 80 / ? + @
• Pattern update setting	s			
• Auto Scaling mode set	ttings			
• Policy synchronization	settings			
<ul> <li>Backup/Restore policy</li> </ul>	·			

- To access, go to Policy settings → Default settings → Operation mode
- The default operation mode of AIWAF-VE is 'Detection.' Click on 'Block' and press 'Apply' to proceed.

APPLICATION INSIGHT WAF									
Monitoring	Log analysis	Report	Policy	settings 🛚	Co	onfigurations			
Default settings a	Admin policy	Domain policy	Policy test						
Apply policy/Cancel 🚊	«	습 Operation mo	ode NEW						
There is a policy that has been changed. Do you want to apply the policy?		Operation mode		O Policy byp	ass	O Detection mode	Block mode		
Apply policy		Bypass target		Request v Header name:Value			: All headers are ap	plied if ti	
Restored to the previous	policies.			[Request/Response] Content-Type:application/vnd.ms.wms-hdr.asfv1					
Click menu title to move to the menu				(Request/     (Request/     (Request/     (Request/	Response) Response) Response)	Content-Type:application Content-Type:application Content-Type:application	on/x-mms-framed on/x-wms-getcontentinfo on/x-wms-LogStats		
<ul> <li>Operation mode N</li> </ul>									
• User authentication				URL Path H	TTP 🗸	://	80 /		
o System overload auto t	ovpass								

• When making changes, you'll see the '**Apply policy/Cancel**' box on the left. Select '**Apply policy**' to save and apply the modified settings.

#### APPLICATION INSIGHT WAF

Monitoring	Log analysis	Report	Policy settings	Configurations				
Default settings N	Admin policy	Domain policy F	Policy test					
<ul> <li>Domain managem</li> <li>Domain policy</li> </ul>	ent	Policy apply/ca	ancel		0			
Default			Don	nain	Changed items			
		Default			0 Case(s)			
		Total count(s) : 1 Case(s)						
		Apply policy	Restored to the previou	s policies.				

- <u>To apply the blocking policy completely</u>, you need to change the **Detect** setting to **Block** for each individual security policy per domain.
- To access, go to **Policy settings** → **Domain policy**
- Click '**Default**' to manage each security policy. (The default page refers to the basic rule settings applied to the web pages users have registered(5-1, 5-2).)

#### APPLICATION INSIGHT WAF

Monitoring	Log analysis	Report	Policy settings	Configurations	
Default settings 😐	Admin policy	Domain policy Po	olicy test		
<ul> <li>Domain management</li> <li>Domain policy</li> </ul>		Applied URL	•	- Rule name         - Use/Not use         All         • Action         All         • Mail         All         •	Search
Default		Batch change use	/not use of policies	Ise  V Apply  · Batch change action of policies Detect  V Apply  F	Policy status summary view
		Vulnerability attack d	letection		× & V
		SQL injection		Rule 1Count(s) Detect	ct 1Count(s) Block 0Count(s)
		LDAP injection		Rule 1Count(s) Detect	ct 1Count(s) Block 0Count(s)
		Cross site script		Rule 1Count(s) Detect	ct 1Count(s) Block 0Count(s)
		Cookie forgery		Rule 1Count(s) Detect	ct 1Count(s) Block 0Count(s)
		CSRF detection		Rule 1Count(s) Detect	ct 1Count(s) Block 0Count(s)
			d detection	Rule 1Count(s) Allow 0Count(s) Detect	ct 1Count(s) Block 0Count(s)
		Malicious file access	s detection	Rule 1Count(s) Detect	ct 1Count(s) Block 0Count(s)
		Command injection	detection	Rule 1Count(s) Detect	ct 1Count(s) Block 0Count(s)
		Directory access de	tection	Rule 1Count(s) Detect	ct 1Count(s) Block 0Count(s)
		⊞ Vulnerable page acc	cess detection	Rule 1Count(s) Detect	ct 1Count(s) Block 0Count(s)
		System file access (	detection	Rule 1Count(s) Deted	ct 1Count(s) Block 0Count(s)
		Web server vulneral	bility detection	Rule 1Count(s) Detect	ct 1Count(s) Block 0Count(s)
		Header vulnerability	detection	Rule 1Count(s) Detect	ct 1Count(s) Block 0Count(s)
		Application vulnerat	bility detection	Rule 1Count(s) Detect	ct 1Count(s) Block 0Count(s)
		Scanner/Proxy/Span	mbot detection	Rule 1Count(s) Detect	ct 1Count(s) Block 0Count(s)

• All default rules are set to 'Detect'. Please click on the rule you want to change.

Mada and Bills and all data stices							54.0.0
vulnerability attack detection							V 1/4 ×
SQL injection					Rule 1Count(s)	Detect 1Count(s)	Block 0Count(s)
Add rule						View	header Apply
🔲 😃 🛛 Rule name	Client IP	Server URL	Unused patterns	Schedule	Explanation	Action Log Mail	Risk Change
이 U SQL Injection	All IPs	All URLs	0 Case(s)	Always		🛡 🗂 🍙	P 2
Total count(s) : 1 Case(s)							
LDAP injection					Rule 1Count(s)	Detect 1Count(s)	Block 0Count(s)
Cross site script					Rule 1Count(s)	Detect 1Count(s)	Block 0Count(s)
🗆 Caalija faraan:					Dula (Count/o)	Detect 10 ount/o)	Disal: 0Count(a)

- The green shield below the Action on the right side of the security rule represents the '**Detect**' mode. Clicking on it will change it to '**Block**'.
- To apply the changes, please click the 'Apply' button.

Successfully applied the policies. Do you want to apply the policies? Apply policy Restored to the previous policies.										
Applied URL		Rule name		Use/Not use All	Action Al	Mail All	•			
- Batch change use/not use o	of policies Use 🗸 Ap	• Batch change ac	tion of policies	Detect						
Vulnerability attack detection	new									
□ SQL injection 🛛							Rule 10			
Add rule										
🔲 😃 Rule name	Client IP		Server URL		Unused patterns	Schedule	Ехр			
SQL Injection	All IPs	All URLs			0 Case(s)	Always				
Total count(s): 1 Case(s)										

• Similar to saving other modifications, click on 'Apply policy' at the top to save your changes.

Applied URL     Sule name     Use/Not use     All     Action     All	✓ • Mail 🛛 All	✓ Risk All	✓ Search	
Batch change use/not use of policies Use      Apply     Batch change action of policies Detect     Apply     Apply			Policy status	summary view
Vulnerability attack detection				♥& ≈
SQL injection		Rule 1Count(s)	Detect 0Count(s)	Block 1Count(s)
LDAP injection		Rule 1Count(s)	Detect 1Count(s)	Block 0Count(s)
Cross site script		Rule 1Count(s)	Detect 1Count(s)	Block 0Count(s)
Cookie forgery		Rule 1Count(s)	Detect 1Count(s)	Block 0Count(s)
CSRF detection		Rule 1Count(s)	Detect 1Count(s)	Block 0Count(s)
🖾 Malicious file unlead dataction	Pulo 1Count/c)	Allow 0Count(c)	Dotact 1Count(c)	Plack (Count/c)

- You'll notice that the SQL injection security rule has been switched from 'Detect' to 'Block'.
- You can refer to page 22 to review actual log data (detection, blocking data).

## 7. Complete Configuration:

#### APPLICATION INSIGHT WAF



• Your configuration is now set. You can monitor web traffic at Monitoring → Dashboard.

## Testing AIWAF-VE: Procedure for Test

If you're looking to conduct a test with AIWAF-VE, follow these steps. Please note that the client (visitor) for this test scenario is designed around the Windows OS.

## Step 1: Redirect Test Traffic to AIWAF-VE:

To direct test client (visitor) traffic to AIWAF-VE, adjust the DNS information using the procedure below. In an actual network setting, you would typically modify the A record or CNAME of the domain name server. However, in this example, we're outlining a process that involves changing the contents of the hosts file.

- Launch Notepad as a Windows administrator.
- In Notepad, navigate to File and choose Open.
- Locate the hosts file path and open it using Notepad.
- Windows hosts file path: C:₩Windows₩System32₩drivers₩etc₩hosts
- Register the IP of AIWAF-VE along with the domain name of the protected web server.
- Example: [AIWAF-VE IP] [Domain] (e.g., 192.168.10.110 www.yourdomain.com)
- Save the hosts file.

## Step 2: Send Sample Traffic to AIWAF-VE:

Generate sample detection traffic from the client (visitor) PC to AIWAF-VE.

- Open an internet browser.
- Enter the following values in the URL address input: URL: http://www.yourdomain.com/?monitorapp=monitorapp

## Step 3: Verify Attack Detection:

Check if the attack is logged in AIWAF-VE's detection log.

#### APPLICATION INSIGHT WAF

Monitoring	Log analysis	Report	Policy settings	Configurations							
Detection log view	Audit log view	View web server sta	itus log								
C <sup>4</sup> All Delete											
Period : 2023-08-16 12:	Period : 2023-08-16 12:51 ~ 2023-08-16 13:21 ×										
• Period O Today	$\bigcirc$ 1 week	○ 1 month	8-16 🔢 12 🗸 : 51 🗸 ~	2023-08-16 🔲 13 🗸 : 21 🗸							
Search Q Down	nload 皆 🛛 Char	t 诀 🛛 Pivot Chart 诀									
Auto Refresh 5 se	C. 🗸										
Attack domain: 0Coun	Attack domain: 0Count(s)   Attacker(Origin IP): 0Count(s)(0Count(s))   Attack count: 0Case(s)										
Time	Client IP	Origin IP Serve	r IP Domain	Detection type							
				There is no data							

- Navigate to: Web UI > Log analysis > Detection log view.
- This procedure provides a concise way to test AIWAF-VE. For more detailed instructions and assistance, consult our user manual or reach out to our support team.

APPLICATION INSIGHT WAF

## Step 3: Verify Attack Detection:

Check if the attack is logged in AIWAF-VE's detection log.

APPLICATION INSIGHT WAF												
Monitoring Log analysis Report Policy settings Configurations												
Detection log view	Audit log view	View web server s	tatus log									
C <sup>*</sup> All Delete	C All Delete											
Period : 2023-08-16 12:	Period : 2023-08-16 12:51 ~ 2023-08-16 13:21 X											
• Period O Today	O1 week	0 1 month 💿 2023-	08-16 📑 12 🗸 : 51 🗸	~ 2023-08-16 📑 13 🗸 : 21 🗸								
Search Q Dow	nload 🗈 🛛 Chart	🚯 Pivot Chart 🚱										
Auto Refresh 5 se	Auto Refresh 5 sec. V											
Attack domain: UCour	Attack domain: 0Count(s)   Attacker(Origin IP): 0Count(s)(0Count(s))   Attack count: 0Case(s)											
Time	Client IP	Origin IP Serv	er IP Domain	Detection type								
				There is no data								

• Navigate to: Web UI > Log analysis > Detection log view.

#### \*Example of Detection Log View(using quick guide's policy setup)

Monitoring	Log analysi	is Re	eport i	Policy settings 🛚	Configurations								
Detection log vie	Detection log view Audit log view View web server status log												
C All Delete													
(Period : 2023-08-22 10:52 ~ 2023-08-22 12:06 <b>x</b> )													
· Period O Today O 1 week O 1 month  O 2023-08-22 III 10 ·: 52 · 2023-08-22 III 12 ·: 06 · · View only pattern detection mode logs · Show only interest logs · · Show only interest logs · · · · · · · · · · · · · · · · · · ·													
Search Q Download B Chart & Pivot Chart &										C Apply search filter			
Auto Refresh	5 sec. 🗸									Search [	15 line(s	s) 🗸	
Attack domain: 1Count(s)   Attacker(Origin IP): 1Count(s)(0Count(s))   Attack count: 10Case(s)													
Time	Client IP	Origin IP	Server IP	Domain	Detection type	Rule name		URL	Risk	Action	Mail	ه	
08-22 10:52:40	112.216.3.62	? None	3.38.96.49	Default	SQL injection	SQL Injection	http://example.com/		- P	•		Q	
08-22 10:52:32	(	? None	3.38.96.49	Default	SQL injection	SQL Injection	http://example.com/		18			Q	
08-22 10:52:12	112.216.3.62	? None	3.38.96.49	Default	Directory access detect	Directory Access	http://example.com/		12			Q	
08-22 10:52:12	(•) 112.216.3.62	? None	3.38.96.49	Default	System file access det	System File Access	http://example.com/		18	•		Q	
08-22 10:52:09	112.216.3.62	? None	3.38.96.49	Default	Character set limits det	CHARSET	http://example.com/		12	•		۹	
08-22 10:52:09	(	? None	3.38.96.49	Default	Cross site script	Cross-Site Scripting	http://example.com/		18			Q	

• You can confirm the detection and blocking results below the 'Action'. In this case, SQL injection has been successfully blocked (indicated by a red shield icon), and other attacks have been detected (indicated by a green shield icon).



MONITORAPP offers further resources more in-depth information and support.

- Support Contact: +1-909-957-1335
- Email: support@monitorapp.com

Copyright © 2024 MONITORAPP, Inc

This user manual is protected by copyright law. Reproduction, public transmission, distribution, translation, or transformation of all or part of this user manual, whether in electronic media or machine-readable form, is prohibited.