

User Manual





Document Control	
Reference	MS_SB/MAN/001
Distribution	Standard
Status	Approved
Version	1.1
Date	01 st Sept 2021

About StrongBox IT

StrongBox IT was founded with the purpose of providing confidence to the businesses against all operational failures. Our vision is to help people and enterprises StrongBox their IT infrastructure in terms of security, performance, Continuous regression, scalability and availability.

Today's production environment is a conduit of varied technologies trying to interact as one unified system. This pushes the operational support team to scale, at times, beyond their capacity to ensure continuous availability of business systems. StrongBox IT compliments the operational support team in their endeavor by helping them validate every change being rolled into production

To address the need of protecting business from IT downtime, StrongBox IT provides security testing, performance testing and regression automation services.





Contents

Where do we stand in the world of internet and innovation?	5
Web Application Firewall – A Quick Introduction	5
What is Modshield SB?	6
Modshield SB – Powerful at heart	7
Purpose of the document	8
Installing Modshield SB VM Image	9
Installing Modshield SB from the AWS Marketplace	
Installing Modshield SB from the Azure Marketplace	
Installing Modshield SB from the GCP Marketplace	23
Setting up a Domain in Modshield SB	26
Adding SSL certificate to Modshield SB	
Adding a Domain to Modshield SB	
Modshield Configuration – Basic Configuration	40
Paranoia Levels	41
Engine Mode	43
Request Limit	
Antivirus Scanning	47
Response Processing	47
Log Policy	
Modshield Configuration – Fine tune your firewall	51
IP Reputation Filters	52
Denial of Service Protection	54
Load Balancer Configuration	57
Data Loss Prevention	62
Adding your own error page	68
Import Logs	69
Access Control	71
Whitelists and Blacklists	71
Geo IP Filter	76
Safe IP	79
Rules Management	82



MODSHIELD^{SB}

Default Rulesets and Rules	82
Custom Rules	85
Log Management	95
View Alerts	95
Blacklist IP	96
Analyse Logs	97
Download Alert Logs	98
View Raw Logs	98
Download Raw Logs	100
Transfer Logs using FTP	102
Log Forwarding	103
Update Modshield	105
Update License	106
Update Threat Intelligence Feeds	106
Modshield Updates	107
Import / Export Configuration	108
References	110



Where do we stand in the world of internet and innovation?

Accelerated digital innovation is a double-edged sword that hangs over the cybersecurity threat landscape. As companies rapidly pursue digital transformation to compete, they can expose more of their business to cyber disruption and theft. The problem is that cyber criminals are innovating in lockstep or, in some cases, at a greater rate.

It's easy to take your eye off the ball given the complexity in both technology innovation and the cybersecurity threat landscape. It's more important than ever to ensure a continued focus on your cybersecurity strategic plan, making adjustments based on the evolving threat landscape so that you are prepared to prevent, detect, and remediate cybersecurity issues.

If this can be achieved by a simple 10-minute process, why wait. Channel years of cybersecurity experience, collective intelligence of world's leading experts and a time-tested product to protect your information and data assets.

Web Application Firewall – A Quick Introduction

A web application firewall (or WAF) filters, monitors, and blocks HTTP traffic to and from a web application. A WAF is differentiated from a regular firewall in that a WAF is able to filter the content of specific web applications while regular firewalls serve as a safety gate between servers. By inspecting HTTP traffic, it can prevent attacks stemming from web application security flaws, such as SQL injection, cross-site scripting (XSS), file inclusion, and security misconfigurations.

A web application firewall is a special type of application firewall that applies specifically to web applications. It is deployed in front of web applications and analyzes bi-directional web-based (HTTP) traffic - detecting and blocking anything malicious. The OWASP provides a broad technical definition for a WAF as "a security solution on the web application level which - from a technical point of view - does not depend on the application itself." According to the PCI DSS Information Supplement for requirement 6.6, a WAF is defined as "a security policy enforcement point positioned between a web application and the client endpoint. This functionality can be implemented in software or hardware, running in an appliance device, or in a typical server running a common operating system. It may be a stand-alone device or integrated into other network components." In other words, a WAF can be a virtual or physical appliance that prevents vulnerabilities in web applications from being exploited by outside threats. These vulnerabilities may be because the application itself is a legacy type or it was insufficiently coded by design. The WAF addresses these code shortcomings by special configurations of rule-sets, also known as policies.

WAFs are not an ultimate security solution, rather they are meant to be used in conjunction with other network perimeter security solutions such as network firewalls and intrusion prevention systems to provide a holistic defense strategy.

MODSHIELD





What is Modshield SB?



- Modshield SB is a web Application Firewall that is powerful and enterprise grade yet affordable and easy to implement
- Modshield SB is custom built using Modsecurity (the most trusted firewall by security engineers) and OWASP CRS (providing adequate coverage to application threats), adding analytics and intuitive configuration elements that are normally cumbersome
- Modshield SB is built for implementation on AWS, Alibaba cloud and as a Virtual machine
- StrongBox IT continuously update the custom rulesets and threat intelligence feeds thereby, eliminating the need for the business to ensure regular updates







Modshield SB – Powerful at heart

A customized implementation of Modsecurity and OWASP Core rule set to protect your web and mobile applications



- Straight through implementation no technical experience required
- Available on AWS, Alibaba and as a Virtual Machine

rulesets and

unlimited custom

rules

SSL Support – included

- Protect unlimited domains and applications
- Continuously updated rule sets included
- Unlimited custom rules included
- Health checks included



Protect multiple

applications and websites



Web site Health Checks

Modshield SB – All the good stuff

<section-header><section-header><section-header><complex-block><image><image><image><complex-block><image><complex-block>





Purpose of the document

The purpose of this document is to help a Modshield user make use of the powerful and extremely useful features that Modshield provides. The document has been divided into sections addressing the basic setup and the advanced fine-tuning options that Modshield provides.

For additional help, please write to ms support@strongboxit.com





Installing Modshield SB VM Image

Step No: 1 Download the VM image from the FTP link provided and upload it to a VM manager. Please allocate a 4 core, 16 GB RAM instance with a minimum of 100 GB of free space. Please ensure that the instance has an active internet connection. Assign a static IP address to this instance if the VM will be accessed externally.

Step No2: Visit http://<Public IP>:5000/modshieldsb_login to access the administrative panel



Enter the provided password in the password field to login.

You should now be greeted with the empty dashboard page as follows

Modshield S	SB × +					
← → C △	① Not secure 52.87.230.33:5000/dash	board		☆	💩 🗧 💿 🗧	G 🔤 🧑 i
Â				2	2 🕂 🕂 A	dministrator 🤨
Dashboard MONITORING	HEALTH CHECK VOID Websites	BLOCKED THREATS O		t!	LOG SIZE 0.0 bytes	']
الم Configuration		Last 1000 Threat	ts Overview (Updated at: 08/	06/2020, 07:23:06)		
Logs	Last 5 days Overview	× Top 5 A	ttacker IP	× Top 10 /	Attack Category	×
Restart ADDONS						
Load Balancer						
() Help						





You will be prompted to change the password on login. Please proceed to the section: Adding a Domain to Modshield SB to continue configuring Modshield SB for the applications that you desire to protect





Installing Modshield SB from the AWS Marketplace

Step No: 1 Visit the marketplace page of the version that better suits your needs (Cloud / BYOL). Click on "Continue to Subscribe" button

	Modshield SB -	Web Applicatio	n Firewall		Continue to Subscribe
A MODSHIELD**	By: StrongBox IT LLC 🗹	Latest Version: Modshield	SB_1.3C		Save to List
	Modshield SB - The first lay applications face Linux/Unix ☆☆☆☆ Free Trial	er of defence against num	erous threats that web and m	obile	Typical Total Price \$0.75/hr Total pricing per instance for services hosted on c5.xlarge in US East (N. Virginia). View Details
Overview	Pricing	U	sage	Support	Reviews

Step No: 2 Read and confirm that you accept the End User Licence Agreement (EULA)

< Product Detail Subscribe

Subscribe to this software

To create a subscription, review the pricing information, and accept the terms for this software. You can also create a long term contract on this page.

Terms and Conditions

StrongBox IT LLC Offer	
By subscribing to this software, you agree to the pricing terms and the seller's <u>End User</u> <u>License Agreement (EULA)</u> ^[2] . You also agree and acknowledge that AWS may share	
information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the <u>AWS Privacy</u>	Accept Terms
Notice C ³ . Your use of AWS services is subject to the <u>AWS Customer Agreement</u> C ³ or other agreement with AWS governing your use of such services.	

Step No: 3 You should see the status as **"Pending"** for a while when AWS processes your request, which should eventually change to the date when you accepted the EULA

You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA) ^C. You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the AWS Privacy Notice ^C. Your use of AWS services remains subject to the AWS Customer Agreement^C or other agreement with AWS governing your use of such services.

Product	Effective date	Expiration date	Action
Modshield SB - Web Application Firewall	8/6/2020	N/A	✓ Show Details





Step No: 4 Click on "Continue to Configuration" button on top right to configure your instance

Modshield SB - Web Application Firewall	Continue to Configuration
Thank you for subscribing to this product! You can now configure your software.	x

Step No: 5 Confirm the Modshield SB version and Region that you want the instance to be deployed, and click the **"Continue to Launch"** button

Configure this software

Choose a fulfillment option below to select how you wish to deploy the software, then enter the information required to configure the deployment.

Delivery Method 64-bit (x86) Amazon Machine Image (AMI)	Ŧ
Software Version	
ModshieldSB_1.3C (Jul 27, 2020)	•
Region	
US East (N. Virginia)	•
Ami id: ami-00195685910009152	
Product code: eztahri69uvi3nfyqyawze8az	





Step No: 5 Confirm the Instance Type, VPC and subnet settings in the following page as per your needs, or you can use the recommended defaults

EC2 Instance Type		¥	Memory: 8 GiB CPU: 16 EC2 Compute Units (4 virtual cores with 4.0 Compute Units each) Storage: EBS storage only Network Performance: Up to 10Gbps
VPC Settings * indicates a default vpc vpc-7a58b507 Create a VPC in EC2 🖸	T	C	
Subnet Settings subnet-d46d89e5 (us-east-1e) Create a subnet in EC2 C [*] (Ensure you are in the selected VPC above)	¥	3	IPv4 CIDR block: 172.31.48.0/20

Step No: 6 Since Modshield SB requires ports 22,80,443,5000 open for access to administrative panel and normal operations, you can either click on **"Create New Based on Seller Settings"** to pre-populate the security group, or configure a new security group as per your requirements

Security Group Settings		
A security group acts as a firewall that contro security group based on seller-recommended	ols the d settin	traffic allowed to reach one or more instances. You can create a new 1gs or choose one of your existing groups. Learn more
Select a security group	٣	c
Create New Based On Seller Settings		



Step No: 7 Enter name and description for the new security group, and click on **"Save"** Button. You can also restrict access to the administrative panel by allowing access only from a particular IP or range of IPs by modifying the Source IP fields at this step

ModebioldSR Security C	roup		
scription	noup		
This is the Security Grou	p with rules for Modshiel	d SB WAF	
Connection Method	Protocol	Port Range	Source (IP or Group)
SSH	tcp	22	Anywhe v 0.0.0.0/0
нттр	tcp	80	Anywhe • 0.0.0.0/0
HTTPS	tcp	443	Anywhe v 0.0.0.0/0
	tcp	5000	Anywhe 🔻 0.0.0.0/0

Step No: 8 Create keypair for the new instance by selecting the **"Create new keypair in EC2"** link which takes you to the Keypair section in EC2

To ensure that no other person has that you created.	as access to your so	oftware, the s	oftware insta	lls on an EC2 ii	nstance with a	an EC2 key pair
Select a key pair	•	C				
Create a key pair in EC2 C [*] (Ensure you are in the region you	wish to launch you	ur software)				

MODSHIELD^{SB}



Step No: 9 Click on "Create new keypair" and give suitable name

Create Key Pair		×
Key pair name:	modshield-sb-keypair	
	Cancel	Create

Step No: 10 Once you click on **"Create"** button in the previous step, save the generated keypair file in PEM format to a safe and secure location

Click the button with the refresh symbol, and select the newly generated keypair from the list. Click on **"Launch"** button to start your instance

Key Pair Settings		
To ensure that no other person has a that you created.	tess to your software, the software installs on an EC2 instance with an EC	C2 key pair
modshield-sb-keypair	• S	
Create a key pair in EC2 🗹		
(Ensure you are in the region you wis	to launch your software)	
		Launch

Your instance should now be deployed to your EC2 console

Launch this software
Congratulations! An instance of this software is successfully deployed on EC2!
AMI ID: ami-00f95e839f0dc9152 (View Launch Configuration Details) You can view this instance on EC2 Console. You can also view all instances on Your Software. Software and AWS hourly usage fees apply when the instance is running and will appear on your monthly bill.
You can launch this configuration again below or go to the configuration page to start a new one.
Configuration Details

Fulfillment Option	64-bit (x86) Amazon Machine Image (AMI) Modshield SB - Web Application Firewall running on c5:xlarge
Software Version	ModshieldSB_1.3C
Region	US East (N. Virginia)
Usage Instructions	





In the next section, we will check on accessing the dashboard, and configuring various domains and related settings

Accessing dashboard

Click on the "EC2 Console" link in previous step to take you directly to the page where your instance is running

Note the Instance ID (which will be the initial password), and Public IP of the WAF instance

Name	 Instance ID 	 Instance Type 	e 👻 Availability Zone	• Instance State	 Status Che 	cks 👻 Alarm Sta	atus Public D	NS (IPv4) 👻 I
	i-0539effbf3	4cfc48c t2.large	us-east-1e	running	2/2 chec	ks None	🍖 ec2-52-8	7-230-33.com
4								•
Instance: i-053	39effbf34cfc48c	Public DNS: ec2-52-87	230-33.compute-1.am	azonaws.com				
Description	Status Checks	Monitoring Tags	Usage Instructions					
	Instance ID	i-0539effbf34cfc48c		Pul	blic DNS (IPv4)	ec2-52-87-230-33. 1.amazonaws.com	.compute-	- 1
	Instance state	running			IPv4 Public IP	52.87.230.33		
	Instance type	t2.large			IPv6 IPs	-		
	Finding	Opt-in to AWS Compute O recommendations. Learn r	otimizer for nore		Elastic IPs			
	Private DNS	ip-172-31-63-119.ec2.inter	nal	A	vailability zone	us-east-1e		
	Private IPs	172.31.63.119		5	Security groups	ModshieldSB_Sec	curity_Group. view	
Sec	condary private IPs			Sci	heduled events	inbound rules, view	w outbound rules nts	

Visit http://<Public IP>:5000/modshieldsb_login to access the administrative panel

Login Modshield SB × +		
← → C ☆ ③ Not secure 52.87.230.33:5000/modshieldsb_lo	ogin 🖈 🥶 🚳 📍 🔯 🔚 🧑) :
MODSHIELD ^{SB} Powered by ModSecurity and OWASP-CRS	Dashboard Login Username Administrator Password	

Enter your instance ID in the password field to login

You should now be greeted with the empty dashboard page as follows





MODSHIELD^{SB}





Installing Modshield SB from the Azure Marketplace

Step 1: Select your preferred plan (either Cloud or BYOL) from the provided dropdown menu, and click **Continue** button

Create	Modshield SB Web Application Firewall (WAF) By StrongBox IT LLC		X I agree to the provider's terms of use and privacy policy and understand that the rights to use this product do not come from Microsoft, unless Microsoft is the provider. Use of Azure Marketplace is governed by separate terms.
Software Pay as yo Pricing:	plan ou Go - Subscription Model First month free, then starting at \$0.58/hour	-	
Details:	All Modshield SB plans are full feature plans supporting multiple applications		Continue

Step 2: Click on Create button to configure various deployment settings

Modshield StrongBox IT LLC	SB Web Application Firewall (WAF) 🛷
	Modshield SB Web Application Firewall (WAF) Save for later StrongBox IT LLC Free trial Select a plan Pay as you Go - Subscription Model Create Start with a pre-set configuration Want to deploy programmatically? Get started





Step 3: Provide name for your new instance and change size if required from the available list

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * i	Azure subscription 1	\sim
Resource group * 🕕	(New) modshieldsb-test_group	\sim
	Create new	
Instance details		
Virtual machine name * 🔅	modshieldsb-test	~
Region * 🛈	(US) East US	~
Availability options i	No infrastructure redundancy required	\sim
Image * 🕡	Pay as you use - Subscription Model - Gen1	\sim
	Browse all public and private images	
Azure Spot instance ()	🔿 Yes 💿 No	
Size * 🕡	Standard_D2s_v3 - 2 vcpus, 8 GiB memory (\$493.48/month)	\sim
	Select size	

Step 4: Configure your login username and authentication method in the next step. NOTE: You can also opt to use the default **modshield** username to simplify user management.

Administrator account	
Authentication type	SSH public key O Password
	Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine.
Username * (i)	modshield
SSH public key source	Generate new key pair
Key pair name *	modshieldsb-test_key 🗸

Step 5: Click on **Review+Create** button to review the final deployment template and click on **Create** button.





Home > Modshield SB Web Application Firewall (WAF) (preview) >

Create a virtual machine

🕑 Val	lidation pas	sed				
Basics	Disks	Networking	Management	Advanced	Tags	Review + create
PRODU	CT DETAII	.S				
Modshield SB Web Application Not covered by credits ① Firewall (WAF) 0.5800 USD/hr by StrongBox IT LLC Terms of use Privacy policy						
Standard D2s v3 Subscription credits apply ① by Microsoft 0.0960 USD/hr Terms of use Privacy policy Pricing for other VM sizes						
TERMS						
By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed						
Create	e		< Previous	Next > Dov	vnload a t	template for automation

Step 6: Save the SSH private key when prompted and click Download private key and create resource button to deploy your instance







In the next section, we will check on accessing the dashboard, and configuring various domains and related settings

Accessing dashboard

Once your new instance is deployed, copy the **Subscription ID**, which would be default password for your Modshield SB instance

Но	ome > Virtual machines >							
5	wirtual machine	Ŕ						×
۶	Search (Ctrl+/)	x 🖉	🗸 Connect 🕞 Start	🤇 Restart 🔲 Stop 🔯 Capture 📋 Delet	te 🕐 Refresh	Share to mobile		
Ņ	Overview	Î	i Advisor (1 of 2): Enabl	le virtual machine replication to protect your application	ns from regional o	outage \rightarrow		
	Activity log	~	Essentials					<u>^</u>
ጵ	Access control (IAM)	Re	source group (change)	: modshieldsb-test group		Operating system	: Linux (ubuntu 18.04)	
4	Tags	Sta	atus	: Running		Size	: Standard D2s v3 (2 vcpus, 8 GiB memory)	
Ð	Diagnose and solve problems	Lo	cation	: East US		Public IP address	: 40.87.104.97	
6.		Su	bscription (change)	: Azure subscription 1	py to clipboard	Virtual network/subnet	t : modshieldsb-test_group-vnet/default	
Se	ttings	Su	bscription ID	: f0d7b1e2-d70e-2eea-a3b1-90352c12e652 🖸		DNS name	: Configure	
22	Networking	Та	gs (change)	: Click here to add tags				
ø	Connect							_
8	Disks	Pi	roperties Monitorir	ng Capabilities Recommendations (2)	Tutorials			
	Size							
۲	Security		Virtual machine			🗟 Networking		
	Advisor recommendations		Computer name	modshieldsb-test		Public IP address	40.87.104.97	
	Extensions		Operating system	Linux (ubuntu 18.04)		Public IP address (II	Pv6) -	
6	Centinuous deliveru		SKU	payg		Private IP address	10.0.1.4	
46	Continuous derivery		Publisher	strongboxitlic1594816423884		Private IP address (IPV6) -	
	Availability + scaling		Agent status	V I Beady		DNS name	Configure	
	Configuration		Agent version	2 2 4 9 2		DNS hame	Compute	
8	Identity		Host	None		💶 Size		
- 11	Properties	-	Proximity placement	N/A		Size	Standard D2s v3	-
4								E F

Visit http://<Public IP>:5000/modshieldsb_login to access the administrative panel





Enter your Azure Subscription ID in the password field to login

You should now be greeted with the empty dashboard page as follows

ĀĒ					■ 3	⊕ ≜ ∎	Administrator 🔋
Dashboard MONITORING	HEALTH CHECK 0/0 Websites	BLOCKED THREATS O	0	TIME SINCE LAST INCIDENT Not Yet!	•	LOG SIZE 0.0 bytes	
		Last 1000 T	hreats Overview (Update	d at: 08/06/2020, 07:23:0	16)		
Logs	Last 5 days Overview	× Top	5 Attacker IP		Top 10 Attac	k Category	
() Restart							
Load Balancer							
(2) Help							

MODSHIELD^{SB}





Installing Modshield SB from the GCP Marketplace

Step 1: Open the GCP Marketplace listing page that suits your licensing model (Cloud / BYOL), and click on the Launch button.



Step 2: Provide a suitable instance name for your new deployment. Change the Deployment Zone and Machine Type if required, while it's recommended to use the deployment template defaults. Disk Size can be increased if logs are to be rotated less frequently or in systems requiring high traffic

Deployment name			Mod
modshieldsb-test-deployme	nt	11	Solut
Zone 🛞			Software
us-central1-b		-	oortinaro
Machine type 🛞			Operating system
4 vCPUs 👻	15 GB memory	Customise	Terms of Servic
Upgrade your account to or Boot Disk	eate instances with up to 96 co	res	By deploying the s with the StrongBox service and the ter the software or se details about any o the limited extent a service expressly is
Boot disk type 🛞			Dy uping this produ
SSD Persistent Disk		•	may be shared wit performance analy
Boot disk size in GB 🔞			Google is providing

dshield SB - Web Application Firewall overview ion provided by StrongBox IT Pvt Ltd

Ubuntu (18.04)

e

offware or accessing the service you are agreeing to comply x IT PvL Ltd terms of service L_{α}^{2} , GCP. Marketplace terms of rms of applicable open source software licences bundled with rvice. Please review these terms and licences carefully for obligations you may have related to the software or service. To an open source software licence related to the software or supersedes the GCP Marketplace Terms of Service, that open cence governs your use of that software or service.

uct, you understand that certain account and usage information h StrongBox IT Pvt Ltd for the purposes of sales attribution, /sis and support. 💿

ng this software or service 'as-is' and any support for this ce will be provided by StrongBox IT Pvt Ltd under their terms of service.



MODSHIELD[™]

Step 3: Click on the Deploy button once all the settings are finalized



Step 4: Select the deployed package overview link in the left pane and open the **Admin Panel URL** from the right pane to launch the administrative console.

- modshieldsb-test-deployment	× modshieldsb-cloud					
modshieldsb-test-deployment has been deployed	Modshield SB - Web Application Firewall Solution provided by StrongBox IT Pvt Ltd					
Overview - modshieldsb-test-deployment	Admin URL http://35.202.172.190.5000/modshieldsb login P					
→ modshieldsb-cloud modshieldsb-cloud.jinja	Instance modshieldsb-test-deployment-vm					
	Instance zone us-central1-b					
modshieldsb-test-deployment-vm vm instance	Instance machine type n1-standard-4					
modshieldsb-test-deployment-tcp-80 firewall	V MORE ABOUT THE SOFTWARE					
modshieldsb-test-deployment-tcp-443 firewall						
modshieldsb-test-deployment-tcp-5000 firewall	Get started with Modshield SB - Web Application Firewall					
	LOG INTO THE ADMIN PANEL 🖄 OPEN DASHBOARD 👻					
	Suggested next steps					
	Dashboard					
	Visit http://:5000/modshieldsb_login The default password for administrative panel is the instance ID Assign a static external IP address to your VM instance 					
	An ephemeral external IP address has been assigned to the VM instance. If you require a static external IP address, you may promote the address to static. Learn more 🖄					





Accessing dashboard

Once your new instance is deployed, copy the **Instance ID**, which would be default password for your Modshield SB instance

	Dashboard Login
MODSHIELD ^{SB} Powered by ModSecurity and OWASP-CRS	Username Administrator Password
	Login

Enter your GCP Instance ID in the password field to login

You should now be greeted with the empty dashboard page as follows

<u>8</u>					M	C ‡	▲ ∎	Administrator 🔋
Cashboard MONITORING	HEALTH CHECK 0/0 Websites	BLOCKED THR O	EATS	TIME SINCE LAST INCIDENT Not Yet!	Ð	ьо О.	s size 0 bytes	
Configuration								
ъ		Last 1	000 Threats Overview (।	Jpdated at: 08/06/2020, 07:23:	06)			
Logs	Last 5 days Overview		Top 5 Attacker IP		Top 10	Attack Ca	itegory	
(j) Restart								
ADDONS								
Load Balancer								
(2) Help								
•	-1		0					





Setting up a Domain in Modshield SB

Step No: 1 To add a domain, login to your Modshield instance.



Step No: 2 Based on your implementation, this could be a VM or a cloud instance

Login ModShield SB × +	- 6 ×
← → C ③ Not secure 3.34.14.172:5000/login	* 🖬 🔍 👍 🚺 🗄
MODSHIELD ^{sb}	Dashboard Login Username Administrator Password Plesse fil in this field Login
Strongboxit_Josepdat ^	Show all





Step No: 3 Before you begin, configure the DNS for your domain to point to the Modshield SB IP address



Step No: 4 Enter your Modshield password and login







Step No: 5 This dashboard will be blank if you are configuring your first website or application

If your domain has a SSL Certificate, you will be required to complete the addition of SSL certificates first. This will later be associated to the domains that you configure in Modshield SB. If you are adding a HTTP application, you can skip the next section and continue from <u>Adding a Domain to Modshield SB</u>.

Adding SSL certificate to Modshield SB

Step no 1: To add SSL certificate click on configuration ->SSL certificate



MODSHIELD





Step 2: Click on Add SSL certificate icon to add your certificate. You can also view, edit and delete your existing certificates.

$\leftrightarrow \ \ni \ {\tt G}$	A Not secure testbo	x.strongboxit.com:	5000/certificate_list							0-7 🟠	=J 🍈 :
🚺 Apps 🕥	New Tab 🛛 🔐 Media Player	> Order History	🖇 IPL Fantasy League	E-RECEIPT OF EXA	鳟 CAT Admit Card 20) 🔇 application form o	of	*	Cther	r bookmarks	📰 Reading list
A							2	÷	≜ 2	Administra	ator 🔋
E Dashboard MONITORING Configuration	SSL Certific	cate						Add Certi	SSL ficate		
Logs	SSL Certificate										
() Restart			SSL Certificate Na	me			Ac	tions			
ADDONS	testbox.strong	ooxit.com				Z Edit X Delete					
В DLP 0											
Help testbox.strongboxit	.com:5000/certificate_list#										

Step 3: SSL Certificate dialog box appears. Click on choose file option in certificate column and upload your certificate. Click on submit.

\leftrightarrow \rightarrow G	A Not secure testbox.stron	ngboxit.com:5000/cer	tificate_list						07	☆ ≕ 💮 :
🔛 Apps 🕥	New Tab 🛃 Media Player 📏 O	Order History 😗 IPL F	Fantasy League	E-RECEIPT OF EXA	🧐 CAT Admit Card 20	S application for	m of	>>	Other bookr	narks 🛛 🔠 Reading lis
<u> </u>										
Ea Dashboard										
MONITORING			SSL Certif	ïcate		×				
Configuration			Certificate	Name Enter :						
Logs			Certificate	Choo	se File No file choser					
() Restart			Private Key	/ Choo	se File No file chose					
ADDONS			SSL Chain	Disabl	e					
Load Balancer										
EE DLP					Close	Submit				
e										
Help										





Step 4: To edit your certificate click on edit icon.

\leftrightarrow \rightarrow C	A Not secure testbox.strongboxit.com	n:5000/certificate_list			아 ☆ 티	è :
👖 Apps S	New Tab 😭 Media Player 📏 Order Histor	😗 🖇 IPL Fantasy League 😗 E-RECEIPT OF EX	A 🧠 CAT Admit Card 20	0 🔇 application form of	» Other bookmarks 🗄 Read	ding list
₩.				8	C 🕂 🚑 Administrator 🔋	
27 Dashboard	SSL Certificate					
MONITORING					Add SSL Certificate	
L ogs	SSL Certificate					
() Restart		SSL Certificate Name			Actions	
ADDONS	testbox.strongboxit.com		I	🖀 Edit 🗙 Delete		
■ D₽						
(2) Help	.com:5000/certificate_list#					

Step 5: SSL Certificate dialog box appears. You can make the necessary changes to the certificate based on your requirements

$\leftrightarrow \ \rightarrow \ G$	A Not secure testbox.strongboxit.com:500	0/certificate_list			아 ☆ 릐 💮 :
Apps 🕥	New Tab 🔮 Media Player > Order History 🖇	IPL Fantasy League 🕤 E-RECEIF	PT OF EXA 🧔 CAT Admit Card 20	application form of	. » 📃 Other bookmarks 🛛 🖽 Reading lis
		SSL Certificate		×	
		Certificate Name	Enter SSL Certificate Name		
		Certificate	Choose File No file chose	n	
		Private Key	Choose File No file chose	n	
		SSL Chain	Disable		
			Close	Submit	





Step 6: You can delete your existing certificate just by simply clicking on the delete icon.

	A Not segure L testbox strangboxit can	v5000/cortificato list				~~~~ =r 🙈 :
				A F F F F F	n 🗖 01	
Apps 🕤	vew lab 👔 Media Player 🍃 Order History) IPL Fantasy League 1 E-RECEIPT OF	- EXA 🥦 CAI Admit Card 20.	🕤 application form of	» 📋 Otr	er bookmarks 📑 Reading list
AH I					€ ⊕ ♠ª	Administrator 📳
22 Dashboard	SSL Certificate					
					Add SSL	
ہ Configuration					Certificate	
Logs	SSL Certificate					
() Restart		SSL Certificate Name			Actions	
ADDONS	testbox.strongboxit.com		I	😰 Edit 🗙 Delete		
■ DĽ ²						
() Help						
testbox.strongboxit	com:5000/certificate_list#					•

Step 7: You can also upload chain SSL certificate by clicking on Add Certificate

$\leftarrow \ \rightarrow \ {\tt G}$	A Not secure testbo	x.strongboxit.com:	5000/certificate_list						0- ☆	=J 🍈 :
🔛 Apps 🕥	New Tab 🚦 Media Player	> Order History	🖇 IPL Fantasy League	• E-RECEIPT OF EXA	🊳 CAT Admit Card 20.	🔇 application form of.		» 📙 O	her bookmarks	🗄 Reading list
る運							⊠ 2		Administra	itor 🔋
273 Dashboard	SSL Certific	cate								
MONITORING								Add SSL Certificate		
Logs	SSL Certificate									
() Restart			SSL Certificate Na	ne			Actio	ons		
ADDONS	testbox.strong	boxit.com			I	🕻 Edit 🗙 Delete				
B DLP										
Help testbox.strongboxi	.com:5000/certificate_list#									

Step 8: SSL dialog box appears. Change the SSL chain from disabled to enabled by selecting from the drop down list box



	SSL Certificate	×			
	Certificate Name				
	Certificate	Choose File No file chosen			
	Private Key	Choose File No file chosen			
	SSL Chain SSL Chain	Enable Choose File No file chosen			
		Close			

Step 9: Click on choose file option from the SSL chain column. Select the required file and then click on ok. Your file name will appear in the SSL chain column. Then click on submit.

	SSL Certificate	×				
	Certificate Name					
	Certificate	Choose File No file chosen				
	Private Key	Choose File No file chosen				
	SSL Chain	Choose File class.jss.txt				
		Close Submit]			

MODSHIELD^{sb}



Adding a Domain to Modshield SB

Step No: 6 To add your domain to Modshield, open the domain configuration option from the configuration menu



Step No: 7 Click on Add domain icon to add the domain.

23 Dashboard	Domain Configuration					
MONITORING					Add domain	Save Changes
L ogs	Domain Configuration					
() Restart	Show 10 entries				Search:	
	Host Name 1	Destination		SSL Support	Firewall Options	
Load Balancer			No data availa	ble in table		
DLP	Showing 0 to 0 of 0 entries				Previo	bus Next







				Administrator	
	Domain Configur	ation	×		
	Host Name	testbox.strongboxit.com			
	Destination IP	34.205.143.207			
	Enable Firewall	Тгие			
	SSL Certificate	testbox.strongboxit.com			
	Terminate SSL	False			
	TLS Version	■ 1.1 ■ 1.2 ■ 1.3			
		Close Sub	nit		

Step No: 9 Enter your domain name in the Host Name.

	Domain Configur	ation	×	
	Host Name	testbox.strongboxit.com		
Configuration	Destination IP	34.205.143.207		
Lega	Enable Firewall	True		
() Rastart	SSL Certificate	testbox.strongboxit.com		
ADDONS	Terminate SSL	False		
Load Batancer	TLS Version	■ 1.1 ■ 1.2 ■ 1.3		
DLP		Close	nit	
Help				





Step No: 10 Add the IP address in which the application or website is hosted

67 SE			
	Domain Configur	ation ×	
	Host Name	testbox.strongboxit.com	
	Destination IP	34.205.143.207	
	Enable Firewall	True	
	SSL Certificate	testbox.strongboxit.com	
	Terminate SSL	False	
	TLS Version	■ 1.1 ■ 1.2 ■ 1.3	
		Close	

Step No: 11 Enabling Firewall will turn on protection for your domain. You can also choose to turn this on later

	Domain Configur	ation	×	
	Host Name	testbox.strongboxit.com		
	Destination IP	34.205.143.207		
	Enable Firewall	True		
	SSL Certificate	testbox.strongboxit.com		
	Terminate SSL	False		
	TLS Version	■ 1.1 ■ 1.2 ■ 1.3		
		Ctose Subr	nit	





Step No: 12 If you are running a HTTP domain, click on Add Domain to complete the configuration

	Domain Configura	ation ×	
	Host Name	testbox.strongboxit.com	
	Destination IP	34.205.143.207	
	Enable Firewall	True	
	SSL Certificate	Disable	
		Close	

Step No: 13 If you have previously added SSL certificates, It will be displayed in the SSL certificate column.

	Domain Configur	ation	×	
	Host Name	testbox.strongboxit.com		
	Destination IP	34.205.143.207		
	Enable Firewall	True		
	SSL Certificate	testbox.strongboxit.com		
	Terminate SSL	Disable testbox.strongboxit.com		
	TLS Version	■ 1.1 ■ 1.2 ■ 1.3		
		Close	nit	




Step No: 14 You can see that the domain is now added to the list of domains

A H				8	s 3 ⊕ ♦ ²	Administrator 🔋
22 Dashboard	Domain Configuration					
MONITORING					Add domain	Save Changes
' L. Logs	Domain Configuration					
() Restart	Show 10 entries				Search:	
	Host Name 1	Destination 11	SSL Support		Firewall Options	î↓
Load Balancer	testbox.strongboxit.com	34.205.143.207	testbox.strongboxit.com	© ON	🖿 TB 🖽 DTb 💽 Eq	it X Delete
	Showing 1 to 1 of 1 entries				Previous	1 Next
😨 Help						
						•

Step 15: To make changes to the domain configuration click on edit icon

$\leftarrow \ \ \rightarrow \ \ C$	A Not secure testbo	x.strongboxit.com:50	000/domain_list					07	☆ 💮 :
🔛 Apps 🕥	New Tab 🔛 Media Player	> Order History	🖇 IPL Fantasy League ฤ	E-RECEIPT OF EXA	🊳 CAT Admit Card 20	application form of	. »	Other bookmarks	📰 Reading list
る道							⊠ 2 ‡	4 Adminis	trator 🔋
n Dashboard	Domain Co	nfiguratio	n						
MONITORING							Add do	omain S Ch	ave anges
Logs	Domain Configu	iration							
() Restart	Show 10 e	entries					Searc	h:	
	Host	Name î	Destination		SSL Support		Firewall Option	ns	t1
Load Balancer	testbox.strongl	boxit.com	34.205.143.207	testbox.	strongboxit.com	© ON	🖿 TB 🖽	DLP 🕑 Edit 🗙 D	elete
⊞ DLP	Showing 1 to 1 c	of 1 entries						Previous 1	Next
() Help									
									-



Step 16: Domain configuration dialog box appears. You can make the required changes to the DNS configuration here.

$\leftarrow \ \ \rightarrow \ \ C$	A Not secure testbox.strongboxit.com:50	00/domain_list			or 🕁 💮 :
Apps 🔇	New Tab 🔛 Media Player 📏 Order History	🖇 IPL Fantasy League 🕤 E-RE	CEIPT OF EXA 🧠 CAT Admit Card 20	application form of	f » 📃 Other bookmarks 🛛 🖽 Reading list
		Domain Configu	uration	×	
		Host Name	testbox.strongboxit.com		
		Destination IP	34.205.143.207		
		Enable Firewall	True		
		SSL Certificate	testbox.strongboxit.com		
		Terminate SSL	False		
		TLS Version	■ 1.1 ■ 1.2 ■ 1.	.3	
			Close	Submit	

Step 17: To incorporate more than one TLS versions on your domain click on edit in the domain configuration section.

$\ \ \in \ \rightarrow \ {\tt G}$	A Not secure testbox	.strongboxit.com:5	000/domain_list					or 🚖 💮 :
🔛 Apps 🕥	New Tab 🔛 Media Player	> Order History	🖇 IPL Fantasy League 📢	E-RECEIPT OF EXA	🊳 CAT Admit Card 20	application form of	»	Other bookmarks 🔠 Reading list
AE							⊠ 2 0 0 4	Administrator
Dashboard	Domain Co	nfiguratio	n					
							Add doma	in Save
Configuration								Changes
Logs	Domain Configu	ration						
() Restart	Show 10 e	ntries					Search:	
	Host I	Name 1	Destination		SSL Support		Firewall Options	τı
Load Balancer	testbox.strongl	ooxit.com	34.205.143.207	testbox.	strongboxit.com	© ON	🖿 TB 📰 DT	P Z Edit × Delete
DLP	Showing 1 to 1 c	of 1 entries						Previous 1 Next
🕑 Help								
								-



Step 18: Domain configuration dialog box appears. In the TLS versions row you can always switch between multiple versions just by clicking the checkbox next to it.

\leftrightarrow \rightarrow C	A Not secure testbox.strongboxi	it.com:5000/domain_list					or 🕁 💮 :
👖 Apps 🕥 N	ew Tab 🔛 Media Player 🗲 Order H	listory 🦻 IPL Fantasy Leagu	e 👔 E-RECEIPT OF EXA	🊳 CAT Admit Card 20	application form o	f » 🛛 🔂 Other bo	okmarks 🛛 🔠 Reading list
		ation Domair	Configuration		×		
		Host Na	ame testbox	k.strongboxit.com			
		Destina	ition IP 34.205	5.143.207			
		Enable	Firewall True				
		SSL Cer	rtificate testbox	k.strongboxit.com			
		Termina	ate SSL False				
		TLS Ver	rsion 🔲 1.1	■ 1.2 ■ 1.3	3		
				Close	Submit		





Modshield Configuration – Basic Configuration

Video Link: <u>https://youtu.be/o-70VKoGsp0</u>

Login to your Modshield cloud instance or Virtual Machine

AE					■ 3	⊕ ≜ ¤	Administrator 🧃
Dashboard MONITORING	HEALTH CHECK 1/1 Websites	V BLOCKED THE	REATS	TIME SINCE LAST INCIDENT 0 D: 0 H: 16 M: 38 S	s 🗘	log size 558.3 KB	.5
Configuration	configuration SSL Certificate Domain Configuration	Last 1	000 Threats Overview (Upd	lated at: 08/27/2021, 10:12:	:07)		
Logs (J) Restart	Firewall Configuration V	×	Top 5 Attacker IP	×	Top 10 Atta	ick Category	×
	RULES MANAGEMENT		19				
Load Balancer	50		10 ·····				
Help testbox.strongboxit.co	om:5000/dashboard≄		1	1.21 ^{61,12} 6.1 ^{57,161,17}			

Select Firewall Configuration from the configuration menu

商量					■ C	⊕ ▲	Administrator 📳
Dashboard MONITORING	HEALTH CHECK 1/1 Websites	✓ BLOCKED THE 110	REATS	TIME SINCE LAST INCIDENT 0 D: 0 H: 16 M: 38 S	•	log size 558.3 KB	
F Configuration	CONFIGURATION SSL Certificate Domain Configuration	Last 1	000 Threats Overview (Updat	ted at: 08/27/2021, 10:12:0)7)		
Logs (j) Restart	Firewall Configuration	×	Top 5 Attacker IP	×	Top 10 Atta	ck Category	×
ADDONS	RULES MANAGEMENT Default Ruleset Custom Ruleset		19				
Ш р.р			5				
Help testbox.strongboxit.c	om:5000/dashboard#		1	10-90 alessen			





This is where you can set various options to fine tune Modhshield.

Modshield S	8 X G pixtr - Google Search	× +						~ -	٥	×
← → C	A Not secure 10.10.171.19:5000/mg_firewall							• •	Guest	:
611				8	ວ	÷	4 2	Administrator	۲	-
2 Dashboard	Manage Firewall									
	Configure Modshield Service							Save Chang	es	
Configuration		Paranoia Level	Paranoia Level 2							
Logs										
() Restart		Select Engine Mode	Detection + Blocking							Ľ
		Request Limit (bytes)	524228							
lin. Load Balancer	مکر ا	File Upload Scanner	Disabled							
E DIP	•	Response Processing	Enabled							
		Log Policy	Log blocked threats							
Help		IP Reputation Filter	Enabled							
		DoS Protection	Disabled							

Paranoia Levels

The first setting, Paranoia level, allows you to choose the tolerance level of the firewall.

Modshield Si	8 × +							~ -	o ×
← → C	A Not secure 10.10.171.19:5000/mg_firewall							0	uest :
Â				8	ວ	÷	•	Administrator	
20 Dashboard	Manage Firewall								
MONITORING	Configure Modshield Service							Save Change	
Configuration		Paranoia Level	Paranoia Level 2						
Logs			Paranoia Level 4 Paranoia Level 3	Í					
() Restart		Select Engine Mode	Paranoia Level 2 Paranoia Level 1						
ADDONS		Request Limit (bytes)	524228						
Load Balancer	ý	File Upload Scanner	Disabled						
.⊞ DLP	•	Response Processing	Enabled						
		Log Policy	Log blocked threats						
(2) Неф		IP Reputation Filter	Enabled						
Ð		DoS Protection	Disabled						





Modshield S	8 × +					~ - O	×
←→C	Not secure 10.10.171.19:5000/mg_firewall					Guest	1
AH I				a 0	•	Administrator 📳	
2 Dashboard	Manage Firewall						
MONITORING	Configure Modshield Service					Save Changes	
Configuration		Paranoia Level	Paranoia Level 2				
Logs							
() Restart		Select Engine Mode	Detection + Blocking				ł
ADDONS		Request Limit (bytes)	524228				
lin. Load Balancer	يو ا	File Upload Scanner	Disabled				
	•	Response Processing	Enabled				
		Log Policy	Log blocked threats				
© Help		IP Reputation Filter	Enabled				
		DoS Protection	Disabled				

We found level 2, the default setting, to be the most effective with the least false positives

Higher the paranoia level, greater is the chance of false positives.

Modshield S	58 × +				~ - O ×
$\leftrightarrow \rightarrow c$	A Not secure 10.10.171.19:5000/mg_firewall				Guest :
Ā				≊ 2 ⊕ ♠	Administrator 📳
Dashboard	Manage Firewall				
	Configure Modshield Service				Save Changes
Configuration		Paranoia Level	Paranoia Level 2	Modify Paranoia Level for Modshield SB Service	
T.L.		Real data in service - More rul	Paranoia Level 4 Paranoia Level 3		
() Restart		Select Engine Mode	Paranoia Level 2 Paranoia Level 1		
		Request Limit (bytes)	524228		
lin. Load Balancer	<u>s</u>	File Upload Scanner	Disabled		
E OLP	•	Response Processing	Enabled		
		Log Policy	Log blocked threats		
(2) Help		IP Reputation Filter	Enabled		
		DoS Protection	Disabled		



Modshield S	+ × 8						~ - ¤ ×
← → C	▲ Not secure 10.10.171.19:5000/mg_firewall						Guest :
AN .				a (; +	۰	Administrator (3)
Dashboard	Manage Firewall						
	Configure Modshield Service						Save Changes
Configuration		Paranoia Level	Paranoia Level 2				
Logs							
() Restart		Select Engine Mode	Detection + Blocking				
		Request Limit (bytes)	524228				
lite. Load Balancer	J.	File Upload Scanner	Disabled				
EE DLP	•	Response Processing	Enabled				
		Log Policy	Log blocked threats				
© Help		IP Reputation Filter	Enabled				
		DoS Protection	Disabled				

We recommend that you try multiple options before you finalise on the one that best suits your need

Engine Mode

	× + Not secure 10.10.171.19:5000/mg_firewall				✓ - □ × Guest :
AN .				≅ 2 ⊕ ♠	Administrator
Dashboard	Manage Firewall				
	Configure Modshield Service				Save Changes
Configuration		Paranoia Level	Paranoia Level 2		
Logs		Real data in service - More rul		Configure the Modshield	
ڻ Restart		Select Engine Mode	Detection + Blocking	service for detecting threats and/or blocking malicious	
ADDONS		Request Limit (bytes)	524228	requests	
Load Balancer	يكر	File Upload Scanner	Disabled		
	•	Response Processing	Enabled		
		Log Policy	Log blocked threats		
Help		IP Reputation Filter	Enabled		
•		DoS Protection	Disabled		

The next setting, Engine Mode, can help when you are trying multiple settings



Modshield SB	× +				~ - 0 ×
← → C	Not secure 10.10.171.19:5000/mg_firewall				Guest :
AT .				■ C + A	Administrator
20 Dashboard	Manage Firewall				
	Configure Modshield Service				Save Changes
Configuration		Paranoia Level	Paranoia Level 2		
Logs			es, some false positives	Configure the Modshield	
() Restart		Select Engine Mode	Detection + Blocking	service for detecting threats and/or blocking malicious	
ADDONS		Request Limit (bytes)	Detection Only Detection + Blocking	requests	
Load Balancer	يو ا	File Upload Scanner	Disabled		
EI DLP	•	Response Processing	Enabled		
		Log Policy	Log blocked threats		
Help		IP Reputation Filter	Enabled		
		DoS Protection	Disabled		
	Configure SafelP				Save Changes
📕 🔎 Туре	here to search 🛛 🕺 🖄 🛛 🖽	0 🔒 🚘 🚳 !	🕽 📴 🥥 🦃 👘 🕐 32°C	Mostly sunny \land 🧒 🖻 🐑 💭	(↓·)) ENG 10:34

The default is Detection and Blocking. Leave this at Detection Only, till you are ready to go live

Detection only, logs all identified threats but does not block them.

Modshield S	58 × +				~ - ¤ ×
$\leftrightarrow \rightarrow c$	A Not secure 10.10.171.19:5000/mg_firewall				Guest :
AT I				≤ 2 ⊕ ♠	Administrator
Dashboard	Manage Firewall				
MONITORING	Configure Modshield Service				Save Changes
Configuration		Paranoia Level	Paranoia Level 2		
Logs			es, some false positives	Configure the Modshield	
() Restart		Select Engine Mode	Detection Only	service for detecting threats and/or blocking malicious	
ADDONS		Request Limit (bytes)	Detection + Blocking	Tequests	
Load Balancer	J.	File Upload Scanner	Disabled		
⊞ D₽	•	Response Processing	Enabled		
		Log Policy	Log blocked threats		
Help		IP Reputation Filter	Enabled		
•		DoS Protection	Disabled		



By enabling detection only you can analyze the events using this, before you instruct the firewall to block all threats.

Modshield S	8 × +					~ - ¤ ×
← → C	A Not secure 10.10.171.19:5000/mg_firewall					Guest :
AN .				a 2	٠	Administrator 📵
Dashboard	Manage Firewall					
	Configure Modshield Service					Save Changes
Configuration		Paranoia Level	Paranoia Level 2			
T.L. Logs			es, some false positives	-		
() Restart		Select Engine Mode	Detection Only			
		Request Limit (bytes)	524228			
lin. Load Balancer	يكر ا	File Upload Scanner	Disabled			
E DLP	•	Response Processing	Enabled			
		Log Policy	Log blocked threats			
Help		IP Reputation Filter	Enabled			
		DoS Protection	Disabled			

This can help in analyzing false postives, especially when you add custom rules or DLP





Request Limit

The next setting, Request limit, is the size of a request that the firewall will process.

Modshield S	+ × 8				~ - 0 ×
$\leftrightarrow \rightarrow c$	A Not secure 10.10.171.19:5000/mg_firewall				Guest :
AH I				⊠ C ÷ ♠	Administrator 3
Dashboard	Manage Firewall				
	Configure Modshield Service				Save Changes
Configuration		Paranoia Level	Paranoia Level 2		
Logs					
() Restart		Select Engine Mode	Detection + Blocking	Configure the maximum size	
		Request Limit (bytes)	524228	of request data that Modshield should scan for	
Load Balancer	J.	File Upload Scanner	Disabled	threats (in bytes)	
E DUP	•	Response Processing	Enabled		
		Log Policy	Log blocked threats		
Help		IP Reputation Filter	Enabled		
		DoS Protection	Disabled		

You can increase this value if you are expecting large attachments to avoid them being blocked

Modshield SE	x +				~ - 🗆 ×
← → C	A Not secure 10.10.171.19:5000/mg_firewall				Guest :
AH I				≡ 2 ⊕ ≜	Administrator 📳
20 Dashboard	Manage Firewall				
	Configure Modshield Service				Save Changes
Configuration		Paranoia Level	Paranoia Level 2		
T.L.					
		Select Engine Mode	Detection + Blocking		
ADDONS		Request Limit (bytes)	524228		
lille. Load Balancer	<u>_</u>	File Upload Scanner	Disabled		
EL DLP		Response Processing	Enabled	service if response data needs to be validated before	
		Log Policy	Log blocked threats	sending to cuent	
O Help		IP Reputation Filter	Enabled		
		DoS Protection	Disabled		





Antivirus Scanning

You have the option to enable or disable antivirus scanning. When enabled, the scanner will detect and prevent malware-infected files before they are uploaded to the application.

6 2				a 3		•	Administrator
20 Dashboard	Manage Firewall						
	Configure Modshield Service						Save Changes
Configuration		Paranoia Level	Paranoia Level 2				
TEL Logs							
() Restart		Select Engine Mode	Detection + Blocking				
		Request Limit (bytes)	524228				
Line Load Balancer	ي	Antivirus Scanner	Enabled	Antivirus S	canner		
		Response Processing	Enabled Disabled				
DLP		Log Policy	Log blocked threats				
(C) Help		IP Reputation Filter	Enabled				
		DoS Protection	Disabled				
	Configure SafelP						Save Changes

Response Processing

You can turn response processing on or off using this setting.

Modshield S	8 × +				~ - a ×
$\leftrightarrow \rightarrow \mathbf{G}$	A Not secure 10.10.171.19:5000/mg_firewall				Guest :
AT .				85 C 🕂 🔺	Administrator (3)
28 Dashboard	Manage Firewall				
MONITORING	Configure Modshield Service				Save Changes
Configuration		Paranoia Level	Paranoia Level 2		
Logs					
() Restart		Select Engine Mode	Detection + Blocking		
ADDONS		Request Limit (bytes)	524228		
Load Balancer	J.	File Upload Scanner	Disabled	Configure the Modshield	
E DLP	•	Response Processing	Enabled	service if response data needs to be validated before	
		Log Policy	Disabled	sending to client	
Help		IP Reputation Filter	Enabled		
•		DoS Protection	Disabled		





If your application responses need not be validated, you can turn this off.

Modshield S	8 × +				~ - 🗆 X
← → C	A Not secure 10.10.171.19:5000/mg_firewall				Guest :
NH N				■ \$ + \$	Administrator 😰
Dashboard	Manage Firewall				
	Configure Modshield Service				Save Changes
Configuration		Paranoia Level	Paranoia Level 2		
Logs					
() Restart		Select Engine Mode	Detection + Blocking		
		Request Limit (bytes)	524228		
inn. Load Balancer	مکر 🔪	File Upload Scanner	Disabled	Configure the Modshield	
E DLP	•	Response Processing	Disabled	service if response data needs to be validated before sending to client	
		Log Policy	Log blocked threats		
Help		IP Reputation Filter	Enabled		
		DoS Protection	Disabled		

Disabling this will give you a higher performance. This is enabled by default

Modshield Si	8 × +				~ - 🗆 ×
$\leftrightarrow \rightarrow c$	A Not secure 10.10.171.19:5000/mg_firewall				Guest :
Â				≤ 2 ⊕ ≜	Administrator (3)
Dashboard	Manage Firewall				
	Configure Modshield Service				Save Changes
Configuration		Paranoia Level	Paranoia Level 2		
Logs					
ڻ ا		Select Engine Mode	Detection + Blocking		
ADDONS		Request Limit (bytes)	524228		
<u>lin</u> Load Balancer	<u>s</u>	File Upload Scanner	Disabled	Configure the Modshield	5
EI DLP	•	Response Processing	Disabled	service if response data needs to be validated before	
		Log Policy	Log blocked threats	senaing to client	
© Help		IP Reputation Filter	Enabled		
		DoS Protection	Disabled		





Log Policy

You can also choose to log only the blocked threats or log everything, based on your requirement

Modshield S	58 × +				~ - 🗆 ×
$\leftrightarrow \rightarrow \ {\tt C}$	A Not secure 10.10.171.19:5000/mg_firewall				Guest :
Ā				≊ 3 ⊕ ≜	Administrator
Dashboard	Manage Firewall				
	Configure Modshield Service				Save Changes
Configuration		Paranoia Level	Paranoia Level 2		
Logs					
() Restart		Select Engine Mode	Detection + Blocking		
		Request Limit (bytes)	524228		
lifn. Load Balancer	<u> </u>	File Upload Scanner	Disabled		
.⊞ ouP	•	Response Processing	Disabled	Configure Modshield service	
		Log Policy	Log blocked threats	to log only malicious requests or every request (Consumes more disk space)	
Help		IP Reputation Filter	Log Everything	(consumes more disk space)	
		DoS Protection	Disabled		

Logging every request and response might be required for certain compliance reasons

Modshield Si	в × +				~ - 🗆 ×
← → C	▲ Not secure 10.10.171.19:5000/mg_firewall				Guest :
AT I				≅ 2 ⊕ ♠	Administrator 🕘
Dashboard	Manage Firewall				
	Configure Modshield Service				Save Changes
Configuration		Paranoia Level	Paranoia Level 2		
Logs					
() Restart		Select Engine Mode	Detection + Blocking		
ADDONS		Request Limit (bytes)	524228		
Load Balancer	Le la construction de la constru	File Upload Scanner	Disabled		
EI DLP	•	Response Processing	Disabled	Configure Modshield service	
0		Log Policy	Log Everything	to log only malicious requests or every request (Consumes more disk space)	
Help		IP Reputation Filter	Enabled		
•		DoS Protection	Disabled		
	R				





Also be aware that log files grow faster when all activity is logged.

Modshield !	58 × +				~ - ¤ ×
$\leftrightarrow \rightarrow \ G$	A Not secure 10.10.171.19:5000/mg_firewall				Guest :
Æ				≊ 2 ⊕ ♠	Administrator 📵
Dashboard	Manage Firewall				
	Configure Modshield Service				Save Changes
Configuration		Paranoia Level	Paranoia Level 2		
Logs					
() Restart		Select Engine Mode	Detection + Blocking		
		Request Limit (bytes)	524228		
Load Balancer	Le la	File Upload Scanner	Disabled		
E DLP	l l	Response Processing	Disabled	Configure Modshield service	
		Log Policy	Log Everything	requests or every request (Consumes more disk space)	
Help		IP Reputation Filter	Enabled		
		DoS Protection	Disabled		

If you are forwarding log entries externally, the forwarded events are also based on this setting

The default setting is to Log only the blocked threats.

Modshield S	8 × +				~ - 🗆 ×
$\leftrightarrow \rightarrow c$	A Not secure 10.10.171.19:5000/mg_firewall				Guest :
AN I				≊ 2 ⊕ ♠	Administrator
Dashboard	Manage Firewall				
MONITORING	Configure Modshield Service				Save Changes
Configuration		Paranoia Level	Paranoia Level 2		
Logs					
(j) Restart		Select Engine Mode	Detection + Blocking		
ADDONS		Request Limit (bytes)	524228		
lds. Load Balancer	J.	File Upload Scanner	Disabled		
E DLP	•	Response Processing	Disabled	Configure Modshield service	
		Log Policy	Log blocked threats	to log only malicious requests or every request	
Help		IP Reputation Filter	Log Everything	(Consumes more disk space)	
Ð		DoS Protection	Disabled		





Please remember to Save Changes for all your settings to take effect

Modshield S	58 × +						~ - O	×
$\leftrightarrow \rightarrow \mathbf{G}$	A Not secure 10.10.171.19:5000/mg_firewall						Guest	:
AH.				8	C	•	Administrator 🔋	Î
Dashboard	Manage Firewall							
	Configure Modshield Service						Save Changes	
Configuration		Paranoia Level	Paranoia Level 2					
Logs								
() Restart		Select Engine Mode	Detection + Blocking					E.
		Request Limit (bytes)	524228					
lán. Load Balancer	\$	File Upload Scanner	Disabled					
E DLP		Response Processing	Enabled					
		Log Policy	Log blocked threats					
() Help		IP Reputation Filter	Enabled					
		DoS Protection	Disabled					

Modshield Configuration – Fine tune your firewall

Video Link: <u>https://youtu.be/rfLHrQibYdc</u>

Select Firewall Configuration from the configuration menu

C Dashboard	- ModShield SB × +				- 0 ×
$\leftarrow \ \rightarrow \ \times$	O Not secure 3.34.14.172:5000/dashboard				🖈 🖸 🛛 🔏 🚺 Paused) :
					🛱 🍂 Administrator 📳
Dashboard MONITORING	WEBSITE HEALTHCHECK 2/3 Websites	BLOCKED THREATS 57932	O D: 0 H	AST INCIDENT 1: 5 M: 27 S	LOG SIZE 1
Configuration	CONFIGURATION Domain Configuration				
Logs	Firewall Configuration	× Top 5 Atta	acker IP	× Top 10 /	Attack Category X
ADDONS	RULES MANAGEMENT				
Load Balancer	Default Ruleset				
	Custom Ruleset				
DLP	20,000				
(i) Restart			II. .		
ee Help	0 20/Apr/20 21/Apr/20 22/Apr/20 23/Apr/20 24		1001 1012010 10 1010 10 1000 10 1000		
Waiting for 3.34.14	.172				· · · · · · · · · · · · · · · · · · ·



								C P
	•	•	L			1		- ³⁶
	•	•			• •		•	•
				_				

IP Reputation Filters

The first setting that we will look at, is IP reputation

Modshield S	B × +				~ - • ×
$\leftrightarrow \rightarrow \mathbf{G}$	A Not secure 10.10.171.19:5000/mg_firewall				Guest :
Ā				⊠ C ⊕ ♠	Administrator
Dashboard	Manage Firewall				
	Configure Modshield Service				Save Changes
Configuration		Paranoia Level	Paranoia Level 2		
TE Logs					
() Restart		Select Engine Mode	Detection + Blocking		
		Request Limit (bytes)	524228		
lite. Load Balancer	مکر ا	File Upload Scanner	Disabled		
E DLP	•	Response Processing	Disabled		
		Log Policy	Log blocked threats		
Help		IP Reputation Filter	Enabled	be from common attackers, spammers, and TOR nodes	
		DoS Protection	Disabled		

This filter blocks all known bad IP addresses, Bots, crawlers and Tor exit nodes

Modshield Si	8 × +				~ - ¤ ×
$\leftrightarrow \rightarrow \mathbf{G}$	A Not secure 10.10.171.19:5000/mg_firewall				Guest :
Ā				8 C 🕂 🔺	Administrator 🕘
Dashboard	Manage Firewall				
MONITORING	Configure Modshield Service				Save Changes
Configuration		Paranoia Level	Paranoia Level 2		
TE Logs					
() Restart		Select Engine Mode	Detection + Blocking		
ADDONS		Request Limit (bytes)	524228		
Load Balancer	J J	File Upload Scanner	Disabled		
EE DLP	•	Response Processing	Disabled		
0		Log Policy	Log blocked threats	Right IPs that are known to	
Help		IP Reputation Filter	Enabled	be from common attackers, spammers, and TOR nodes	
•		DoS Protection	Disabled		



MODSHIELD^{SB}

Modshield is continuously updated with threat intelligence feeds to ensure efficient detection

Modshield Si	8 × +				~ - ¤ ×
← → C	A Not secure 10.10.171.19:5000/mg_firewall				Guest :
AN I				■ C + A	Administrator (3)
Dashboard	Manage Firewall				
	Configure Modshield Service				Save Changes
Configuration		Paranoia Level	Paranoia Level 2		
T.L. Logs					
() Restart		Select Engine Mode	Detection + Blocking		
		Request Limit (bytes)	524228		
Load Balancer	<u></u>	File Upload Scanner	Disabled		
E DLP		Response Processing	Disabled		
		Log Policy	Log blocked threats		
© Help		IP Reputation Filter	Disabled	Block IPs that are known to be from common attackers, spammers, and TOR nodes	
		DoS Protection	Disabled		

The default setting is "Disabled". Enable it to have real time threat protection

Modshield SB	× +				~ - ¤ ×
← → C	A Not secure 10.10.171.19:5000/mg_firewall				Guest :
AH.				≊ 2 ⊕ ♠	Administrator 📳
20 Dashboard	Manage Firewall				
MONITORING	Configure Modshield Service				Save Changes
Configuration		Paranoia Level	Paranoia Level 2		
TEL Logs					
() Restart		Select Engine Mode	Detection + Blocking		
ADDONS		Request Limit (bytes)	524228		
Load Balancer	مکر	File Upload Scanner	Disabled		
EL DLP	~	Response Processing	Disabled		
		Log Policy	Log blocked threats		
Help		IP Reputation Filter	Enabled	Block IPs that are known to be from common attackers, spammers, and TOR nodes	
•		DoS Protection	Enabled Disabled		

There might be a slight compromise on performance when this filter is enabled





Denial of Service Protection

The next setting that we will talk about is DoS protection

This setting is disabled by default

Modshield SE	* * +				~ - ¤ ×
← → C	▲ Not secure 10.10.171.19:5000/mg_firewall				Guest :
611				≝ C ÷ ♠	Administrator 📵
Dashboard	Manage Firewall				
	Configure Modshield Service				Save Changes
Configuration		Paranoia Level	Paranoia Level 2		
Logs					
() Restart		Select Engine Mode	Detection + Blocking		
		Request Limit (bytes)	524228		
Load Balancer	يو ا	File Upload Scanner	Disabled		
	•	Response Processing	Disabled		
		Log Policy	Log blocked threats		
Help		IP Reputation Filter	Disabled		
		DoS Protection	Disabled	Enable/Disable Protection against Denial-of-Serive (DoS) Attacks	e

Enabling this setting will also require you to define the parameters for identification

Modshield SB	× +					~ - O	×
← → C	Not secure 10.10.171.19:5000/mg_firewall					Guest) I
A B Dashboard	Manage Firewall			■ C +	•	Administrator 🧃	Î
MONITORING	Configure Modshield Service					Save Changes	
Configuration		Paranoia Level	Paranoia Level 2				
Logs							
() Restart		Select Engine Mode	Detection + Blocking				
ADDONS		Request Limit (bytes)	524228				
Load Balancer	مکر 🔪	File Upload Scanner	Disabled				
	•	Response Processing	Disabled				
		Log Policy	Log blocked threats				
Help		IP Reputation Filter	Disabled				
Ð		DoS Protection	Disabled	Enable/Disable F against Denial-o	Protection of-Serivce		
			Enabled Disabled	(Dos) Atta			



Modshield SB × + - o × ← → C ▲ Not secure | 10.10.171.19:5000/mg_firewall Guest : Administrator -Configure Modshield Service . Configuratio () Restart Detection + Blocking Request Limit (bytes) Disabled Log Policy Log blocked threats Disabled

You will have to define these parameters so that a DoS attack can be identified accordingly

For example, 100 requests from an IP, within 60 seconds, can be considered as an attack

Let's see how we set this in the firewall and block that IP for 600 seconds or 10 minutes

The first setting, Burst Time slice, defines the time period for identification

Modshield SB	× +						~ -	o ×
← → C /	Not secure 10.10.171.19:5000/mg_firewall						00	Suest :
MONITORING	Configure Modshield Service			a 2	÷	•	Administrator	۲
Configuration		Paranoia Level	Paranoia Level 2					
Logs								
() Restart		Select Engine Mode	Detection + Blocking					
ADDONS		Request Limit (bytes)	524228					
Load Balancer		File Upload Scanner	Disabled					
EE DLP		Response Processing	Disabled					
		Log Policy	Log blocked threats					
© Неф		IP Reputation Filter	Disabled					
$\mathbf{\bullet}$		DoS Protection	Enabled					
		Burst Time Slice	60					
		Counter Threshold	100					
		Block Timeout	600					
								^

MODSHIELD





Here, the count of the number of similar requests will be reset every 60 seconds

The threshold defines the maximum allowable number of requests within the burst time slice

Modshield SB	× +							~ -	
← → C	Not secure 10.10.171.19:5000/mg_firewall							• e	Guest :
MONITORING	Configure Modshield Service			8	ø	÷	•	Administrat	or 📵 🔒
Configuration		Paranoia Level	Paranoia Level 2						
Logs									
() Restart		Select Engine Mode	Detection + Blocking						
ADDONS		Request Limit (bytes)	524228						
Load Balancer		File Upload Scanner	Disabled						
EL DLP	2	Response Processing	Disabled						
-		Log Policy	Log blocked threats						
Help		IP Reputation Filter	Disabled						
		DoS Protection	Enabled						
		Burst Time Slice	60						
		Counter Threshold	100						
		Block Timeout	600						

If there are 100 similar requests within 60 seconds, it is identified as an attack

The IP from which the requests arise is then blocked for the timeout interval

Modshield S8	× +					~ -	٥	×
← → C ▲	Not secure 10.10.171.19:5000/mg_firewall					• e	Guest	:
VasnoGaru						l'anne	-	^
MONITORING	Configure Modshield Service			89 i.	· ••	Administrate	r 🤓	
Configuration								
_		Paranoia Level	Paranoia Level 2					
Logs								
U		Select Engine Mode	Detection + Blocking					
Restart								
ADDONS		Request Limit (bytes)	524228					
Load Balancer		File Upload Scanner	Disabled					
		Personal Processing	Disabled					
	C 4	Response Processing	UISADLEU					
		Log Policy	Log blocked threats					
(i) Help		ID Paputation Filter	Disabled					
		in Reputation Filter	Uisauteu					
		DoS Protection	Enabled					
		Purst Time Clice	60					
		Burst Time Suce	80					
		Counter Threshold	100					
		Plack Timeout	600					
		Block Timeout						

Any IP sending out more than 100 requests within 60 seconds gets blocked for 600 seconds.





Load Balancer Configuration

Video Link: https://youtu.be/GxNRHpZsaxY

Login to Modshield and select Domain Configuration from the Configuration menu

AT .				8	c + 🔹	Administrator
Dashboard MONITORING	HEALTH CHECK 1/1 Websites	BLOCKED THREATS 110	O D: 0 H	16 M: 38 S	LOG SIZE 558.3 KB	12
Configuration	CONFIGURATION SSL Certificate	Last 1000 Threats	Overview (Updated at: 08/27	7/2021, 10:12:07)		
Logs ()	Domain Configuration	× Top 5 Att.	acker IP	х Тор	10 Attack Category	×
ADDONS	Access fritering Rules management Default Ruleset	19				
Load Balancer	Custom Ruleset	10				
	50	5				
Help testbox.strongboxit.co	om:5000/dashboard#					

Click on the LB button next to the domain for which you want to configure the load balancer.

Modshield S	8 × +					~ - ¤ ×
← → C	A Not secure 10.10.171.19:5000/domain_list					Guest :
AH					8 C + 4	Administrator 🕘
Deshboard	Domain Configuration					
MONITORING					Add domain	Save Changes
۲ ۲ Logs	Domain Configuration					
ل) Restart	Show 10 entries				Search:	
ADDONS	Host Name T	Destination	SSL Support		Firewall Options	
Load Balancer	testphp.vulnweb.com	44.228.249.3	False	© ON		Edit × Delete
DLP	Showing 1 to 1 of 1 entries				Previo	us 1 Next
e Help						





The Load Balancer Options option allows you to set the different modes of load balancing

Modshield S	+ × 8				~ - ¤ ×
$\leftrightarrow \rightarrow \mathbf{G}$	A Not secure 10.10.171.19:5000/load_balancer/testphp.vulnweb.com				Guest :
AH.				■ 2 +	Administrator
Dashboard	Load Balancer				
MONITORING	Domain: testphp.vulnweb.com		Add	Save	Cancel
Configuration	Load Balancer Options			By Requests 🕶	Persistence Disabled -
() Restart	Show 10 entries			Search:	
ADDONS	Destinati	on IP Address		Actions	
Load Balancer	44.228.249.3			8 ↑↓	
E DLP	Showing 1 to 1 of 1 entries				Previous 1 Next
© Help					
•					

Choose the mode that best suits your requirement

Modshield !	58 × +					~ - 🗆 ×
← → C	▲ Not secure 10.10.171.19:5000/load_balancer/testphp.vulnw	eb.com				Guest :
AH				a	■ 2 ⊕	Administrator
2 Dashboard	Load Balancer					
MONITORING	Domain: testphp.vulnweb.com		Add	:	Save	Cancel
Configuration Logs	Load Balancer Options				By Requests -	Persistence Disabled -
() Restart	Show 10 entries				By Requests By Traffic	
ADDONS		Destination IP Address			By Busyness	11
Load Balancer	44.228.249.3			× ↑↓	Hear Wear	
ELP	Showing 1 to 1 of 1 entries					Previous 1 Next
(C) Help						
•						





To enable persistence which is disabled by default, simply click on the field and choose enable.

Modshield S	8 × +				\sim – \Box \times
$\leftarrow \ \rightarrow \ G$	A Not secure 10.10.171.19:5000/load_balancer/testphp.vulnweb.com				Guest :
AH I				■ 2 + 4	Administrator
Dashboard	Load Balancer				
	Domain: testphp.vulnweb.com		Add	Save	Cancel
Logs	Load Balancer Options			By Requests 🔻	Persistence Enabled -
() Restart	Show 10 entries			Search:	Enabled Disabled
ADDONS	Destination	IP Address		Actions	
Load Balancer	44.228.249.3		×↑	4	
E DLP	1.2.3.4		×↑	•	
0	Showing 1 to 2 of 2 entries				Previous 1 Next
Help					
\mathbf{b}					
📕 🔎 Тур	be here to search 🥂 📶 O 🖽 💽 🐂	🚖 O () 🕸 🗗 O		🕥 30°C Cloudy \land 🍘 🖗 🕯	18:14 ■ d× ENG 03-08-2022

Click on the Add button to add all the IP addresses that host the application

Modshield S	58 × +				~ - O ×
← → C	A Not secure 10.10.171.19:5000/load_balancer/testphp.	ulnweb.com			Guest :
A				■ 2 +	Administrator
2 Dashboard	Load Balancer				
MONITORING	Domain: testphp.vulnweb.com		Add	Save	Cancel
Configuration	Load Balancer Options			By Requests 🕶	Persistence Disabled 👻
() Restart	Show 10 entries			Search	
ADDONS		Destination IP Address		Actions	
Load Balancer	44.228.249.3			第 个少	
E DLP	Showing 1 to 1 of 1 entries				Previous 1 Next
(C) Help					





Enter the IP address in the destination IP field and click on Add

Modshield	sa × +					~ - O ×
$\leftrightarrow \rightarrow \ C$	A Not secure 10.10.171.19:5000/load_balancer/testphp.vuln	web.com				Guest :
A						
Dashboard						
Honertannea						
Lagi		Add Configuration	n			
(!) Restart		Host Name	testphp.vulnweb.	com		
Actorialis Im. Coad Batancer		Destination IP	1.2.3.4			
(1) 01.P				Close		
e Hegi						

This adds the IP address to the list of servers the application is hosted on

Modshield SB	x +			~ - 🗆 ×
← → C	Not secure 10.10.171.19:5000/load_balancer/testphp.vulnweb.com			Guest :
AH .			■ 3 +	Administrator
23 Dashboard	Load Balancer			
MONITORING	Domain: testphp.vulnweb.com	Add	Save	Cancel
Logs	Load Balancer Options		By Requests 👻	Persistence Disabled •
(j) Restart	Show 10 entries		Search	
ADDONS	Destination IP Address		Actions	7.1
lin. Load Balancer	44.228.249.3		ж ↑↓	
	1.2.3.4		× ↑↓	
	5.6.7.8		* **	
© Help	Showing 1 to 3 of 3 entries			Previous 1 Next
$\mathbf{\mathbf{e}}$				





Repeat this for all the IP addresses that you wish to add and then click on Save

Modshield S	8 × +			~ - O ×
← → C	Not secure 10.10.171.19:5000/load_balancer/testphp.vulnweb.com			Guest :
Ā			■ 2 +	Administrator
23 Dashboard	Load Balancer			
MONITORING	Domain: testphp.vulnweb.com	Add	Save	Cancel
Configuration	Load Balancer Options		By Requests 👻	Persistence Disabled 🔻
ڻ Restart	Show 10 entries		Search:	
ADDONS	Destination IP Address		Actions	
lin. Load Balancer	44.228.249.3		× ↑↓	
E	1234		X 个小	
	5.6.7.8		* ↑↓	
© Help	Showing 1 to 3 of 3 entries			Previous 1 Next
•				

You have now successfully configured the load balancer

To Verify the change, Open the Domain Configuration from the configuration menu

Â					ı 0 4 4	Administrator
Cashboard MONITORING	HEALTH CHECK 1/1 Websites	BLOCKED THREATS 110		SINCE LAST INCIDENT D: 0 H: 16 M: 38 S	D 100 SIZE 558.3 K	в 'Д
الم Configuration	CONFIGURATION SSL Certificate	Last 1000 Three	ats Overview (Updated at	08/27/2021 10:12:07)		
Logs	Domain Configuration	× Top 5	Attacker IP	× To	op 10 Attack Category	×
() Restart	Access Filtering					
	Default Ruleset					
DLP		10 -				
() Help	50 com:5000/deshboard#	1	Barry Barrier , Bergerice , Darson	a the second		





Notice that the destination for the domain has been changed to LB instead of a single IP address

Modshield S	58 × +					~ - • ×
$\leftrightarrow \rightarrow \ G$	A Not secure 10.10.171.19:5000/domain_list					Guest :
AN I					≥ 2 4 4	Administrator 🔋
Pashboard	Domain Configuration					
					Add domain	Save Changes
TE. Logs	Domain Configuration					
() Restart	Show 10 entries				Search:	
ADDONS	Host Name	1 Destination	SSL Support		Firewall Options	
iin. Load Balancer	testphp.vulnweb.com	LB	False	© ON	LB DLP	Z Edit X Delete
E DLP	Showing 1 to 1 of 1 entries				Prev	vious 1 Next
() Help						
•						

You can also do this from the Load Balancer menu. Simply choose the domain from the menu and configure as shown earlier. Do not forget to Save your changes

Data Loss Prevention

Video Link: https://youtu.be/GxNRHpZsaxY

To Configure Data Loss Prevention, Open the domain configuration from the configuration menu







Click on the DLP button next to the domain for which you would like to configure the DLP

Modshield S	4 × 82					~ - ¤ ×
← → C	A Not secure 10.10.171.19:5000/domain_list					Guest :
δΞ.					≥ 2 + 4	Administrator 😨
20 Dashboard	Domain Configuration					
					Add domain	Save Changes
TE Logs	Domain Configuration					
() Restart	Show 10 entries				Search:	
ADDONS	Host Name 1	Destination	SSL Support		Firewall Options	
lin. Load Balancer	testphp.vulnweb.com	44.228.249.3	False	© ON		Edit × Delete
	Showing 1 to 1 of 1 entries				Pr	revious 1 Next
© Help						
•						

Click on Add to instruct Modshield on the format of data that is considered as sensitive

Modshield S	58 × +						~ - ¤ ×
$\leftrightarrow \rightarrow \ G$	A Not secure 10.10.171.19:5000/dlp/testphp.vulnweb.com						Guest :
AH.					■ 3	⊕ ♠	Administrator 🧿
Dashboard	Data Leak Prevention (DLP)						
	Domain: testphp.vulnweb.com		A	dd 📃	Save		Cancel
2	DLP Settings						
Logs	Show 10 entries					Search:	
Restart	Description	Regex		Action		Actions	
		No data av	vailable in table				
Load Balancer	Showing 0 to 0 of 0 entries						Previous Next
DLP							
(i) Help							
\mathbf{O}							





Enter a name for your rule to easily identify what this data pattern is for...

Modshield	SB × +				~ - ¤ ×
$\leftarrow \ \ \rightarrow \ \ C$	A Not secure 10.10.171.19:5000/dlp/testphp.vulnweb.com				Guest :
Dashboard					
MONITORING Ju Configuration		DLP Rule			
Logs		Host Name	testphp.vulnweb.com		
Ċ,		Description			
ADDONS		Regex			
Lina Ralancer		Need help? Refer here			
		Action	Deny + No Log		
e e			Close		

I am going to restrict all responses that have a master card number

Modshield SE	× +				~ - 🗆 ×
$\leftarrow \ \ \rightarrow \ \ C$	A Not secure 10.10.171.19:5000/dlp/testphp.vulnweb.com				Guest :
る調					
Dashboard					
		DLP Rule			
Logs		Host Name	testphp.vulnweb.com		
() Restart		Description	Mastercard Credit Card Number		
ADDONS		Regex	Enter Regex for DLP Rule		
Load Balancer		Need help? Refer here			
		Action	Deny + No Log		
DLP					
🕞 Help			Close Add		



Provide the regex for the data format. Please ensure that the regex is accurate. All responses from the application that contains Mastercard numbers will be filtered

Modshield S	58 × +				\sim – \Box \times
$\leftrightarrow \rightarrow c$	A Not secure 10.10.171.19:5000/dlp/testphp.vulnweb.com				Guest :
お理				= 0 ÷	Administrator
Dashboard					
		DLP Rule			Cancel
Logs		Host Name	testphp.vulnweb.com		
(j) Restart		Description	Master Card Credit Card		Actions
		Regex	^5(1-5)/d{14}\$		
Load Balancer		Action	Deny + No Log		Previous 1 Next
DLP					
© Help			Close		
•					

You can choose to allow the response and not store sensitive information in the log files or you can choose to block the response itself. In both cases this data will not be logged

← → C ▲ Not secure 10.10.171.19:5000/dlp/testphp.vulnweb.com	🛛 🕒 Guest 🗄
- A11 = 0	4) Administrator
Data Leak Prevention (DLP)	
An and testphp vulnweb.com Save	
DLP Settings Host Name testphp.vulnweb.com	
Show 10 entries Description Master Card Credit Card	
Description In Regex ^5(1-5)/d{14}\$	
Need help? Refer here	
Action Allow + No Log	
Close Add	



				 	_	51
10	D	5	Н			9

I choose the block all responses with sensitive data

Modshield S	58 × +				~ - 🗆 ×
$\leftarrow \ \rightarrow \ G$	A Not secure 10.10.171.19:5000/dlp/testphp.vulnweb.com				Guest :
51					
Dashboard					
		DLP Rule			
Logs () Restart		Host Name	testphp.vulnweb.com		
		Description	Master Card Credit Card		
ADDONS		Regex	^5(1-5)∧d{14}\$		
Line Long Relations		Need help? Refer her			
		Action	Deny + No Log		
DLP			Allow + No Log		
€ Help			Close Add		

Click on Add to add this condition. You can repeat this to add any number of filters for DLP

Modshield 5	8 × +			~ - ¤ ×
$\leftrightarrow \rightarrow \mathbf{G}$	A Not secure 10.10.171.19:5000/dlp/testphp.vulnweb.com			🛛 😫 Guest 🕕
Cashboard				
Handraman P		DLP Rule		
		Host Name	testphp.vulnweb.com	
U) Featuret		Description	Master Card Credit Card	
Antoenies		Regex	^5(1-5)/d{14}\$	
las, Lond thatmen		Need help? Refer here		
		Action	Deny + No Log	
.D.C.				
e Him			Close Add	





Click on Save to save this change

Modshield 5	58 × +				~ - O ×
← → C	A Not secure 10.10.171.19:5000/dlp/testphp.vulnweb.com				Guest :
Ā				≥ 2 0	Administrator
2 Dashboard	Data Leak Prevention (DLP)				
MONITORING	Domain: testphp.vulnweb.com		Add	Save	Cancel
Configuration	DLP Settings				
Logs (j)	Show 10 entries			Sear	ch:
Restart	Description	11 Regex	1. Action		Actions 11
	Master Card Credit Card	^5(1-5)/d{14}\$	Deny + No Log	8 17 4	
	Showing 1 to 1 of 1 entries				Previous 1 Next
(i) Help					
\mathbf{O}					

Erroneous Regex might block responses that are safe. Please ensure accuracy of the regex used.

Dashboard - ModShield S8 x G credit card regex - Google Searci x +								
$\leftarrow \ \rightarrow \ G$	A Not secure 3.34.14.172:5000/dlp/really-not-	a-valid-domain.com		¥	2 🖸 🝳 者 🕖 Paused) :			
N E					🔎 Administrator 💿			
Dashboard	Data Leak Prevention (D	DLP)						
MONITORING				Save	Cancel			
Configuration	DLP Settings	▲ WARNING						
Logs	Show 10 🗢 entries	Modifying this section is NOT recomment what you are trying to do. Mis-configurat system unstable and potentially irrecover	ded unless you know ion may make the able.	Searc	h:			
		Are you sure to continue?		11 Actions	н. -			
			No Yes -					
					Previous 1 Next			

You can also set the DLP rules using the DLP option in the left menu.





Adding your own error page

Step 1: To add a custom error page click on configuration ->firewall configuration

Dashboard MONITORING	HEALTH CHECK 0/0 Websites	~	BLOCKED THE 1	REATS	TIME SINCE LAST INCIDENT 0 D: 0 H: 1 M: 30 S	Ø	log size 6.9 KB	
۶	CONFIGURATION				l	· · · · ·	l	
Configuration	SSL Certificate		Last 1	000 Threats Overview (Ur	odated at: 08/27/2021. 13:22	:07)		
	Domain Configuration							
Logs	Firewall Configuration	N	×	Top 5 Attacker IP	×	Top 10 Atta	ack Category	×
() Restart	Access Filtering							
	RULES MANAGEMENT			4				
	Default Ruleset							
Load Balancer	Custom Ruleset			3				
DLP	1							

Step 2: click on choose file from the customization menu

Licensing			Save Changes
	License Key Status: ACTIVATED Your license is managed b	00000-00000-00000-000000 y your Cloud Service Provider.	
Customization			Save Changes
\$	Error Page	Choose File No file chosen	

Step 3: You can choose your pre-designed custom error page and upload it. Click on save changes and your custom error page will now be shown every time a request is blocked by Modshield SB

	four ucense is managed by your Ctobb Service Provider.				
Customization		Save Changes			
¢°,	Error Page Choose File DrumStickApp	html			





Import Logs

If you migrating between two instances of Modshield SB and would like to import the logs from the first instance to the second, please follow the below steps.

STEP 1:To import logs click on configuration-> firewall configuration



STEP 2: In the firewall configuration page click on import from file in the import log section

Customization				8	÷	4 2	Administrator
\$	Error Page Cho	ose File No file chosen					
Update, Backup/Restore							
t.	Download update: Update Modshield Manage Modshield Configuration: (Import Configuration	Lupdate Threat In	el ion				
Import Logs							
<u>t</u>	±	mport from file					1





STEP 3: Once you have imported the logs it is being processed and can be viewed in the log section

2 Dashboard	← Back Alerts Log		■ 3	⊕ ≜ 2	Administrator 📳
	The Modshield log files were las	t processed at 08/27/2021, 13:12:07. Current log size is 863.0 bytes.			
Configuration	Events Log				
Logs	Show 10 entries			Search:	
ADDONS	Timestamp î↓	Host 1↓	Attacker IP	Rule ↓ ID ↑↓	Rule Message î↓
Load Balancer	27/Aug/2021:13:00:07 +0000	34.207.167.99	45.95.168.133	910110	Request from Malicious Client (Known Bad IP address)
(2) Help	27/Aug/2021:13:00:07 +0000	34.207.167.99	45.95.168.133	920350	Host header is a numeric IP address
	27/Aug/2021:13:00:07 +0000	34.207.167.99	45.95.168.133	910110	Request from Malicious Client





Access Control

Video Link: https://youtu.be/281NONeWLrg

Whitelists and Blacklists

Access filtering allows us to set conditional access to a website or a web application



This is done by using a set of whitelists or blacklists.

Modshield !	sa × +		~ - O X
← → C	A Not secure 10.10.171.19:5000/acl		Guest :
A			😂 💭 💠 🌲 🛛 Administrator 💽
Dashboard	Access Filtering		testphp.vulnweb.com 👻 Save
Configuration	Whitelist	Blacklist	GeolP Filtering
Ξ	Enter IP address (comma separated):	Enter IP address (comma separated):	Select mode: ● Whitelist ● Blacklist ● None
Logs (J)			Selected Countries:
ADDONS			
Load Balancer			
E DLP			Select the country:
0			Nothing selected *





Modshield allows you to restrict IPs, IP ranges and countries. You can specify this for each domain

Modshield	SB × +			~ - 🗆 ×
← → C	A Not secure 10.10.171.19:5000/acl			Guest :
AH.			≊ & + ≜	Administrator (2)
Dashboard	Access Filtering		testphp.vulnweb.com 👻	Save
Configuration	Whitelist	Blacklist	GeolP Filtering	
Logs U Restart ADDONS Load Balancer DLP	Enter IP address (comma separated):	Enter IP address (comma separated):	Select mode: • Whitelist • Blacklist Selected Countries: Select the country: Nothing selected *	• None
(C) Help			*	
•				

To begin, select the domain for which you would like to restrict access

Modshield S	58 × +		~	- 0 ×
← → C	A Not secure 10.10.171.19:5000/acl			G uest :
AN .			≅ \$ ⊕ ♠ ^	dministrator 📳
2 Dashboard	Access Filtering		testphp.vulnweb.com	Save
MONITORING			AVAILABLE DOMAINS	
y	Whitelist	Blacklist	testphp.vulnweb.com ⁹ Filtering	
Configuration	Enter IP address (comma separated):	Enter IP address (comma separated):	Select mode:	
Logs			• Whitelist • Blacklist • N	ione
ψ			Selected Countries:	
Restart				
ADDONS				
Load Balancer				
DLP			Select the country:	
			Nothing selected 👻	
(C) Help				




Whitelists allow traffic only from t	the IPs mentioned in the list. All other IPs are blocked

Modshield S	58 × +			~ - O ×
← → C	A Not secure 10.10.171.19:5000/acl			Guest :
Ā			≥ 2 ⊕	Administrator
20 Dashboard	Access Filtering		testphp.vulnweb.com	✓ Save
	Whitelist	Blacklist	GeolP Filtering	
Logs	Enter IP address (comma separated):	Enter IP address (comma separated):	Select mode: • Whitelist • Blacklis Followed Countries:	t 🔍 None
() Restart			Selected Countries.	
ADDONS				
DLP			Select the country:	rted *
) Help				
\bullet				

Blacklists on the other hand, allow traffic from all IPs other than the ones in the list

Modshield S	58 × +				~ - ¤ ×
$\leftrightarrow \rightarrow \ G$	▲ Not secure 10.10.171.19:5000/acl				Guest :
6 <u>8</u>				≥ 2 + 4	Administrator 📳
673 Dashboard	Access Filtering		testphp.vulnwi	eb.com 🔹	Save
Configuration	Whitelist	Blacklist		GeoIP Filtering	
TE. Logs	Enter IP address (comma separated):	Enter IP address (comma separated):		Select mode: • Whitelist • Blacklist	O None
() Restart ADDONS				Selected Countries:	
Load Balancer					
DLP				Select the country: Nothing selected	
© Help					
•					





At any given point, you can only have one of these enabled

Modshield S	SB × +		~ - 0 ×
$\leftrightarrow \ \ \rightarrow \ \ C$	A Not secure 10.10.171.19:5000/acl		🛛 😁 Guest 🗄
AI			😂 🗘 💠 🌲 Administrator 📳
Dashboard	Access Filtering		testphp.vulnweb.com
MONITORING	Whitelist 🦲	Blacklist	GeolP Filtering
U Restart ADDONS	Enter IP address (comma separated):	Enter IP address (comma separated):	Select mode: • Whitelist • Blacklist • None Selected Countries:
			Select the country:
Help			

Turn on the Whitelist and enter the IP address that should be whitelisted

Modshield !	SB × +					~ - 0 ×
← → C	A Not secure 10.10.171.19:5000/acl					Guest :
AH.				= 0	÷ + +	Administrator 🔋
Pashboard	Access Filtering		testphp.vulnweb.co	om	•	Save
	Whitelist	Blacklist	Ger	oIP Filtering		
E.	Enter IP address (comma separated):	Enter IP address (comma separated):	Sel • \	lect mode: Whitelist	 Blacklist 	None
Logs () Restart ADDONS	121.23.43.55		Sel	lected Countries		
DLP			Set	lect the country: N	lothing selected 👻	
Help						





Add additional IPs separated by comma

Modshield !	58 × +		~ - D X
← → C	A Not secure 10.10.171.19:5000/acl		🛛 😁 Guest 🗄
AN I			🖾 📿 💠 🌲 🛛 Administrator 🔋
Dashboard	Access Filtering	te	stphp.vulnweb.com 👻 Save
	Whitelist	Blacklist	GeolP Filtering
Configuration	Enter IP address (comma separated): 121.23.43.55,121.23.43.55	Enter IP address (comma separated):	Select mode: • Whitelist • Blacklist • None Selected Countries:
B DLP			Select the country: Nothing selected >
Help			

Turning on the Blacklist will automatically disable the whitelist. Add IP addresses to this list in the same way as you did for a whitelist

v	- 🛛 🗙
	Guest :
≥ 2 + ▲	Administrator 📳
testphp.vulnweb.com 👻	Save
Blacklist GeolP Filtering	
Enter IP address (comma separated): Select mode:	
● Whitelist ● Blacklist ●	None
Selected Countries:	
Select the country:	
121.23.43.55 Select d Countries: Select the country: Nothing selected ▼	None





Geo IP Filter

Similarly, you can all restrict IPs from a country or countries using the Geo IP filter.

Modshield 5	58 × +		~ - a ×
← → C	A Not secure 10.10.171.19:5000/acl		Guest :
AN I			🖾 📿 🕂 🎄 🛛 Administrator 📳
(7) Dashboard	Access Filtering		testphp.vulnweb.com - Save
	Whitelist	Blacklist	GeolP Filtering
Logs	Enter IP address (comma separated):	Enter IP address (comma separated):	Select mode: ● Whitelist ● Blacklist ● None Selected Countries:
() Restart ADDONS			
Load Balancer			
Ш рцр			Select the country:
(C) Help			
\bullet			

You can choose either to blacklist or whitelist countries

Modshield 5	58 × +			~ - O ×
← → C	A Not secure 10.10.171.19:5000/acl			Guest :
A			≅ 2 ⊕ ♠	Administrator
Dashboard	Access Filtering		testphp.vulnweb.com 👻	Save
	Whitelist	Blacklist	GeoIP Filtering	
T.Logs	Enter IP address (comma separated):	Enter IP address (comma separated):	Select mode: • Whitelist • Blacklist	None
() Restart			Selected Countries:	
ADDONS Im Load Balancer				
Ш DLP			Select the country:	
(i) Help				
•				





Select the countries that you would like to add to your list

Modshield	58 × +				~ - 🗆 ×
$\leftrightarrow \ \ \rightarrow \ \ G$	A Not secure 10.10.171.19:5000/acl				Guest :
A				≅ C ⊕ ♠	Administrator 🕘
2) Dashboard	Access Filtering	l	testphp.vulnw	eb.com 🔹	Save
	Whitelist	Blacklist		GeoIP Filtering	
Logs () Restart ADDONS Im Load Balancer	Enter IP address (comma separated):	Enter IP address (comma separated):		Select mode: • Whitelist • Blacklist Selected Countries:	• None
E				Select the country:	
Help					

You can choose any number of countries to be added to this list

Modshield S	58 × +		~	- 0 ×
$\leftrightarrow \ \ \rightarrow \ \ G$	▲ Not secure 10.10.171.19:5000/acl			Guest :
AN .			≊ 2 ⊕ ≜	Administrator 📳
Dashboard	Access Filtering		testphp.vulnweb.com	Save
	Whitelist	Blacklist	Atghanistan Atbania Atgeria	
Logs	Enter IP address (comma separated):	Enter IP address (comma separated):	✓ American Samoa I Andorra I Angola	
ن Restart			Anguilla Antarctica	* *
			 Antigua and Barbuda Argentina Armenia 	
Load Balancer			Tuba	
			Anguilla, Antarctica	
(C) Help				





You can also disable all lists and save the settings to preserve the lists.

$ \begin{tabular}{lllllllllllllllllllllllllllllllllll$	58 × + Not secure 10.10.171.19:5000/ad			✓ - □ × Guest :
Ā			≅ C + +	Administrator 😰
Dashboard	Access Filtering		testphp.vulnweb.com	Save
	Whitelist	Blacklist	GeoIP Filtering	
Configuration Logs Restart ADDONS Load Bolancer	Enter IP address (comma separated): 1.1.1.1 2.2.2.2	Enter IP address (comma separated): 121.23.43.55,121.23.43.55	Select mode: • Whitelist • Blacklist Selected Countries: AI,AQ Select the country:	• None
© Help			Anguilla, Antarctica	

You are not required to remove the entries. This makes it easier to enable the same settings later

Modshield !	sa × +			~ - ¤ ×
← → C	A Not secure 10.10.171.19:5000/acl			Guest :
AN I				🔤 😂 🕂 🌲 🛛 Administrator 📳
Dashboard	Access Filtering		testphp.vulnw	veb.com 👻 Save
Configuration	Whitelist	Blacklist		GeoIP Filtering
	Enter IP address (comma separated):	Enter IP address (comma separated):		Select mode:
Logs		121.23.43.55,121.23.43.55		Whitelist Blacklist None Selected Countries:
ADDONS				AI,AQ
E DLP				Select the country:
(C) Help				Anguitta, Antarcuca
•				





Safe IP

Another setting that provides IP specific access is called a Safe list (Safe IP)

Safe list is found in the firewall configuration menu item



Scroll down to the Safe IP section

Modshield SB	× +						~ -	\Box ×
← → C ▲	Not secure 10.10.171.19:5000/mg_firewall						• •	Guest :
Configuration		Paranoia Level		8 (. 4		Administrator	
Logs								
() Restart		Select Engine Mode	Detection + Blocking					
ADDONS		Request Limit (bytes)	524228					
lin. Load Balancer	مکر ا	File Upload Scanner	Disabled					
EI DLP	•	Response Processing	Enabled					
		Log Policy	Log blocked threats					
Help		IP Reputation Filter	Enabled					
\bullet		DoS Protection	Disabled					
	Configure SafelP					ĺ	Save Chang	es
	6.8 .	Domain	testphp.vulnweb.com					
	₽₽ ₿	Allowed IP						
								^



Modshield SB	× +						~ - 🗆 ×
← → C ▲	Not secure 10.10.171.19:5000/mg_firewall						Guest :
EI DLP				-	¢ €	•	Administrator 📵
		Log Policy	Log blocked threats				
Hetp		IP Reputation Filter	Enabled				
•		DoS Protection	Disabled				
	Configure SafelP						Save Changes
		Domain	testphp.vulnweb.com				
	4 48	Allowed IP	11.1.1				
	Licensing						Save Changes
		License Key	KEMLQ-BJYEW-CQUYR-ISXDM				
	.≡	Status: TRIAL - ACTIVATED	f deux				
		Tour currrent ucense expires in	o days.				

You can specify Safe IPs for each of the domain that you manage

Modshield will turn off the rules processing for all traffic from this IP address alone

Modshield SB	× +					~ - O	×
< → C ▲	Not secure 10.10.171.19:5000/mg_firewall					Gue 🖯 Gue	est :
() Restart		Select Engine Mode		a c	•	Administrator)
ADDONS		Request Limit (bytes)	524228				
🕍 Load Balancer	J.	File Upload Scanner	Disabled				
EI DLP	•	Response Processing	Enabled				
		Log Policy	Log blocked threats				
Help		IP Reputation Filter	Enabled				
		DoS Protection	Disabled				
	Configure SafelP					Save Changes	Ľ
		Domain	testphp.vulnweb.com				
	19 8	Allowed IP	testphp.vulnweb.com demo.testfire.net				
	Licensing					Save Changes	
							^

MODSHIELD^{SB}





It is important to ensure that the safe IP is not blocked by any whitelist or blacklist settings

As always, please save changes for the settings to take effect

Modshield SB	× +						~ - i	J ×
\leftrightarrow \rightarrow C \blacktriangle	Not secure 10.10.171.19:5000/mg_firewall						0 9	uest
E DUP		Response Processing	Enabled	e 3	÷	•	Administrator	<u>۹</u>
		Log Policy	Log blocked threats					
C Help		IP Reputation Filter	Enabled					
		DoS Protection	Disabled					
	Configure SafelP						Save Changes	
	\$ °	Domain	testphp.vulnweb.com					
		Allowed IP	1.1.1.1					
	Licensing						Save Changes	
	⊥ ≡	License Key	KEMLQ-BJYEW-CQUYR-ISXDM					
		Status: TRIAL - ACTIVATED						
		Your currrent license expires in 6 days.						
								Ŷ,





Rules Management

Video Link: <u>https://youtu.be/qp1VvIu4oOs</u>.

Modshield has a built-in set of rules that enable effective protection against all common attacks

6 2				-	o ⊕ ♠■	Administrator (2)
Dashboard MONITORING	HEALTH CHECK 1/1 Websites	BLOCKED THREATS 110		INCE LAST INCIDENT	D LOG SIZE 558.3 KB	.5
الم Configuration	CONFIGURATION SSL Certificate	Last 1000 Thr	eats Overview (Updated at:	08/27/2021, 10:12:07)		
Logs () Restart	Domain Configuration	X Top !	5 Attacker IP	× To	p 10 Attack Category	×
ADDONS	rules management Default Ruleset					
Lood Balancer	Custom Ruleset					
Help	50		and and and and	-		

Default Rulesets and Rules

To view and configure the default set of rules that are provided, open the default ruleset from the configuration menu

Modshield S	SB	x +					~ -	
$\leftarrow \ \rightarrow \ {\tt G}$	A Not see	ure 10.10.171.19:5000/rules_view					• •	Guest
AH I			a	s 3	÷	٠	Administrate	or 🔋
Dashboard	← Ba	Configure Rules					Save Cha	anges
MONITORING								Toggle
Configuration		SCANNER-DETECTION						•
() Restart	•	PROTOCOL-ATTACK						~
ADDONS		LOCAL FILE INCLUSION (LFI)						~
EI DLP		REMOTE FILE INCLUSION (RFI)						~
Petp		REMOTE CODE EXECUTION (RCE)						~
•		PHP						~
		NODEIS						



MODSHIELD^{SB}

Expand the ruleset by clicking on it. You can see the number of rules enabled in that set\\

Modshield SB	× +	~ - 🛛 ×
← → C ▲	Not secure 10.10.171.19:5000/rules_view	Guest :
A	≊ <i>C</i> + +	Administrator
23 Dashboard	←Back Configure Rules	Save Changes
		Enable ALL Toggle
Configuration	SCANNER-DETECTION	•
لون Restart	PROTOCOL-ATTACK	~
ADDONS im Load Balancer	LOCAL FILE INCLUSION (LFI) Enabled Rules: 4/4 Configure	~
Ш р.р	Identifies users trying to include a file that would be local to the webserver that they should not have access to. Exploiting this type of attack can lead to the web applie being compromised.	cation or server
Help	C REMOTE FILE INCLUSION (RFI)	~
		~

You can choose to disable the rulesets as a whole

Modshield SB	x + ~	- 🗆 ×
← → C ▲	Not secure 10.10.171.19:5000/rules_view	□ (Guest) :
AN I	📼 C 🕂 🌲 🗎 Ad	ministrator 📳
20 Dashboard	Configure Rules	ave Changes
		ALL Toggle
Configuration	SCANNER-DETECTION	•
Logs () Restart	PROTOCOL-ATTACK	~
ADDONS	LOCAL FILE INCLUSION (LFI) Enabled Rules: 4/4 Configure Identifies users trying to include a file that would be local to the webserver that they should not have access to. Exploiting this type of attack can lead to the web application being compromised.	• or server
	REMOTE FILE INCLUSION (RFI)	~
	REMOTE CODE EXECUTION (RCE)	~





or you can click on configure which then lists all the rules in that ruleset

Modshield SB	x +				~ - O	×				
← → C ▲	Not secure 10.10.171.19:5000/rules_view				Gues	st :				
A	8	C		٠	Administrator 🧧					
Dashboard	←Back Configure Rules				Save Changes					
MONITORING						le				
Configuration	C SCANNER-DETECTION				~					
Logs () Restart	PROTOCOL-ATTACK				•					
ADDONS	Enabled Rules: 4/4 Configure Identifies users trying to include a file that would be local to the webserver that they should not have access to. Exploiting this type of attack can lead to the web application or server being compromised.									
Help	REMOTE FILE INCLUSION (RFI)				~					
					~					
						٦.				

You can choose to enable or disable individual rules as well as all the rules as whole using Disable ALL or Enable ALL

Modshield SB	× +	×	~ - • ×
← → C	Not secure 10.10.171.19:5000/rules_view/930		Guest :
A B		■ 2 + ▲	Administrator 🧿
Dashboard	← Back Configure "LOCAL FILE INCLUSION (LFI)"		Save Changes
Configuration	Directory Traversal Attacks - Encoded Payloads		
Logs	Directory Traversal Attacks - Decoded Payloads		
ADDONS	C OS File Access		
Load Balancer EE DLP	C Restricted File Access		
eð Help			
•			





Once done, click on Save Changes to update the rule configurations

Modshield SB	× +				~ -	
\leftrightarrow \rightarrow C \blacktriangle	Not secure 10.10.171.19:5000/rules_view/930				00	Guest
Ā		8	C	•	Administra	itor 💿
Dashboard MONITORING	← Back Configure "LOCAL FILE INCLUSION (LFI)"				Save C	nanges Toggle
Configuration	Directory Traversal Attacks - Encoded Payloads					
Logs (i) Restart	Directory Traversal Attacks - Decoded Payloads					
	OS File Access					
Load Balancer	Restricted File Access					
ල Help						

Custom Rules

You can add custom rules using the custom ruleset menu in the configuration

A.				8	₽ ⊕ ♠	Administrator 🔋
Dashboard MONITORING	HEALTH CHECK 1/1 Websites	BLOCKED THREATS 110		ICE LAST INCIDENT 0 H: 16 M: 38 S	LOG SIZE 558.3 KB	.5
Configuration	CONFIGURATION SSL Certificate	Last 1000 Threats	: Overview (Updated at: 0	8/27/2021, 10:12:07)	- 1	
Logs ()	Domain Configuration	× Top 5 At	tacker IP	х Тор	10 Attack Category	×
ADDONS	Access Hittening Rules Management Default Ruleset					
Load Balancer	Custom Ruleset					
	50					
Help testbox.strongboxi	.com:5000/dashboard#	1	P	a shall		





The rules wizard makes it easy for you to add a simple custom rule

Modshield S	58 × +		~ - O ×
← → C	A Not secure 10.10.171.19:5000/custom_rules		Guest :
Ā		■ 2 +	Administrator
23 Dashboard	Custom Ruleset		
MONITORING		Rules Wizard	Save
Configuration	Custom Ruleset		
() Restart			
ADDONS			
			4
0			
Hep			

Enter a unique rule ID, a name and choose the phase in which the rule should be applied

Modshield	158 × +			~ - 🗆 ×
$\leftrightarrow \ \ \rightarrow \ \ C$	A Not secure 10.10.171.19:5000/custom_rules			Guest :
が見				
Dashboard				
нонстанина				
Configuration		Step 1 - Add Cus	tom Rule ×	
Logi		Rule ID	001	
(i) Heritart		Rule Name	Test Rule	
Antenias		Phase	Request Header	
Lood Shatarreer		Rule Description		
			Close Next	
(inter-				





Modshield applies the rules based on the phase in which it is defined

Modshield S	8 × +			~ - ¤ ×
$\leftrightarrow \rightarrow c$	▲ Not secure 10.10.171.19:5000/custom_rules			Guest :
				Administrator
				Save
		Step 1 - Add Cus	tom Rule X	
		Rule ID	001	
		Rule Name	Test Rule	
		Phase	Request Header	
		Rule Description		
			Close	×

Request header, Body, and Response header, Body are the phases in Modshield

Modshield S	58 × +			~ - O ×
$\leftrightarrow \rightarrow \ G$	A Not secure 10.10.171.19:5000/custom_rules			Guest :
33				Administrator 2
Cashboard				
HONITORING				
Configuration		Step 1 - Add Cus	tom Rule ×	
A regre		Rule ID	001	
U Restort		Rule Name	Test Rule	
Appolis		Phase	Request Header	
in Losd Shanner		Rule Description	Request Header Request Body Response Header Response Body	
0			Close Next	





Choose the phase in which this rule should be applied

Modshield SB	× +			~ - ¤ ×
$\leftrightarrow \rightarrow c$	Not secure 10.10.171.19:5000/custom_rules			Guest :
		Step 1 - Add Cust	tom Rule ×	
		Rule ID	001	
		Rule Name	Test Rule	
		Phase	Request Header	
		Rule Description		
			Close	

Enter the description. This will be stored as a Message in the log file. Click next

Modshield 5	sa × +			~ - O ×
$\leftrightarrow \rightarrow \ C$	A Not secure 10.10.171.19:5000/custom_rules			Guest :
ED Dashboard				
ноноания				
Configuration		Step 1 - Add Cus	tom Rule ×	
Lagu		Rule ID	001	
U) Restort		Rule Name	Test Rule	
Antochis		Phase	Request Header	
jan. Level Hatanear		Rule Description	Enter Rule Description	
DLP.			100 - 100 (mmmm)	
			Close	
Nation 1				





Choose the parameter that the rule is applied on

Modshield SB × +	PERF_RULES	* · · · · ×
← → C ▲ Not secure 10.10.171.19:5000/custom_rules	PERF_SREAD PERF_SWRITE	Guest :
ALL CONTRACTOR OF CONTRACTOR O	QUERY_STRING REMOTE_ADDR REMOTE_HOST REMOTE_PORT	🔳 📿 🕂 🔺 Administrator 3
Custom Ruleset	REMOTE_USER REQBODY_ERROR REQBODY_ERROR_MSG REQBODY_PROCESSOR REQUEST_BASENAME	Rules Wizard Save
Contiguation Custom Ruleset	REQUEST_BODY REQUEST_BODY_LENGTH REQUEST_COOKIES REQUEST_COOKIES_NAMES REQUEST_FILENAME	×
U Brazer	REQUEST_HEADERS REQUEST_HEADERS_NAMES	
Abbova Im.	ARGS	
Cad Burner	Previo	IS Next
- O Hay		

In step 3, select the operation that has to be performed on this parameter

Modshield	sa × +				~ - O ×
$\leftrightarrow \ \ \rightarrow \ \ C$	▲ Not secure 10.10.171.19:5000/custom_rules				Guest :
が通					Administrator
Dashboard					
P					Save
Centiguration		Step 3 - Add Cu	stom Rule		
U U Festart		Rule Operator	beginsWith beginsWith		
Aniperies		Value	contains containsWord		
ins. Leond Statistics EEL DLF		Rule Action	detectSQLi detectXSS endsWith fuzzyHash eq ge		
0 100			geol.ookup gsbl.ookup gt inspectFile ipMatch ipMatchF ipMatchFromFile le lt		





Enter the value against which this parameter has to be compared

Modshield Si	8 × +			~ - O ×
$\leftrightarrow \ \ \rightarrow \ \ C$	A Not secure 10.10.171.19:5000/custom_rules			Guest :
200				
Dashboard				
		Step 3 - Add Cus	tom Rule X	
		Rule Operator	contains	
Adopties		Value	Alert	
les Lond Batancer		Rule Action	Allow Requests	
(III (DUP)			Previous Add Rule	
e Helpi				

and define the action when the rule matches.

Modshield S	+ × 8			~ - 🗆 ×
$\leftrightarrow \rightarrow c$	▲ Not secure 10.10.171.19:5000/custom_rules			Guest :
10				
Dashboard				
HONITERINE Je Destination				
		Step 3 - Add Cu	stom Rule ×	
U) Firstert		Rule Operator	contains	
ACCOUNT		Value	Alert	
los Concl. Bat intern		Rule Action	Allow Requests Allow Requests Denv Requests	
a.#			Block Requests	
ій. нар				
(2)				





I choose to deny all requests that match the criteria defined

Modshield Si	8 × +			~ - ¤ ×
$\leftrightarrow \rightarrow \ G$	A Not secure 10.10.171.19:5000/custom_rules			Guest :
		Step 3 - Add Cus	tom Rule X	
		Rule Operator	contains	
		Value	Alert	
		Rule Action	Deny Requests	
			Previous Add Rule	

Click on Add rule

Modshield	58 × +			~ - 🗆 X
$\leftrightarrow \rightarrow \ G$	A Not secure 10.10.171.19:5000/custom_rules			Guest :
石田				Administrator
Dashboard				
нонгалия.				Save
Configuration		Step 3 - Add Cus	stom Rule ×	
() Restart		Rule Operator	contains	
Anipolius		Value	Alert	
ins. Lond Belation		Rule Action	Deny Requests	
E . DP			Previous Add Rule	
e rea				





You will see the rule displayed in this text box. You can modify the rule here and hit save.

Modshield S	x +		~ - O ×
← → C	▲ Not secure 10.10.171.19:5000/custom_rules		Guest :
AN .		≡ 2 ‡	Administrator
2 Dashboard	Custom Ruleset		
MONITORING		Rules Wizard	Save
Logs	Custom Ruleset		
() Restart ADDONS	SecRule REQUEST_BODY "@contains Alert" "id:999992001, phase:2, deny, msg:'Modshield Custom rule (Test Rule)"		
Load Balancer			
DLP			
() Неф			
•			

Mistakes in the custom rule can adversely affect the working of the firewall.

Modshield SB	× +		~ - o ×
← → C ▲	Not secure 10.10.171.19:5000/custom_rules		Guest :
A			
Deshboard			
нонганна. "р			
Configuration		▲ WARNING ×	
U Westert Antonia		Modifying this section is NOT recommended unless you know what you are trying to do. Mis-configuration may make the system unstable and potentially irrecoverable.	
Lood Balancar		Are you sure to continue?	





You can also write your custom rule here directly instead of using the wizard.

Modshield !	8 x +		~ - 🗆 ×
← → C	▲ Not secure 10.10.171.19:5000/custom_rules		Guest :
ai i		≅ 3 ⊕	Administrator
Dashboard	Custom Ruleset		
MONITORING		Rules Wizard	Save
Configuration	Custom Ruleset		
Logs			
() Restart	SecRule REQUEST_BODY "@beginsWith Alert" "id:999992001, phase:2, deny, msg:'Modshield Custom rule (Test Rule)"		
ADDONS			
Load Balancer			
e Help			
$\mathbf{\bullet}$			

To remove a custom rule, select the rule and delete it. Save Changes

Modshield	58 × +		~ - 🗆 ×
$\ \ \leftarrow \ \ \rightarrow \ \ C$	▲ Not secure 10.10.171.19:5000/custom_rules		Guest :
が強		≥ 2 +	Administrator
23 Dashboard	Custom Ruleset		
MONITORING		Rules Wizard	Save
	Custom Ruleset		
() Restart	SecRule REQUEST_BODY "@beginsWith Alert" "id:999992001, phase:2, deny, msg:Modshield Custom rule (Test Rule)"		
ADDONS			
Load Balancer			
⊞ DLP			
(2) Help			
•			





This will remove the custom rule from the firewall.

Modshield S	58 × +		~ - O ×
← → C	▲ Not secure 10.10.171.19:5000/custom_rules		Guest :
Â		s 2 ÷ 4	Administrator
20 Deshboard	Custom Ruleset		
MONITORING		Rules Wizard	Save
Configuration	Custom Ruleset		
Logs			
() Restart			
ADDONS			
Load Balancer			
⊞ DLP			
6			
Help			
$\mathbf{\mathbf{b}}$			

You can create as many custom rules as you need





Log Management

Video Link: https://youtu.be/TxLWpckvluo

Modshield makes it very easy to analyze events and whole log files written by the firewall

Modshield SB	× +						~ - ¤ ×
← → C	A Not secure 10.10.171.19:5000/fw_log	l.					Guest :
AN .						⊠ C ‡	Administrator
20 Dashboard	← Back Alerts Log						✤ Download Alert Logs
ا بر Configuration	Events Log						
Logs	log management View Alerts					Search	ĸ
() Restart	View Raw Log mp ∏ Manage Log	Host 💷	Request line 👘	Remote Address	Rule Id 🖽	Message	Rule Message 👘
ADDONS	29/Jul/2022:09:27:20 +0000	testphp.vulnweb.c om	POST /userinfo.php HTTP/1.1	10.10.171.23	941380	AngularJS client side template injection detected	Warning. Pattern match "{{-*?}}" at ARGS:urname.
	03/Aug/2022:09:26:19 +0000	testphp.vulnweb.c om	POST /userinfo.php HTTP/1.1	10.10.171.23	942370	Detects classic SQL injection probings 2/3	Warning. Pattern
() Help	03/Aug/2022:09:26:19 +0000	testphp.vulnweb.c om	POST /userinfo.php HTTP/1.1	10.10.171.23	942260	Detects basic SQL authentication bypass attempts 2/3	Warning. Pattern
	03/Aug/2022:09:26:19 +0000	testphp.vulnweb.c om	POST /userinfo.php HTTP/1.1	10.10.171.23	942130	SQL Injection Attack: SQL Tautology Detected	Warning. Pattern
	03/Aug/2022:09:26:19 +0000	testphp.vulnweb.c om	POST /userinfo.php HTTP/1.1	10.10.171.23	942130	SQL Injection Attack: SQL Tautology Detected	Warning. Pattern

View Alerts

Click on View alerts from the Logs menu. This gives you a list of all threats blocked by Modshield

Modshield SE	8 × +						~ - O ×
← → C	A Not secure 10.10.171.19:5000/fw_log						Guest :
AH .						≊ 2 ‡	Administrator
Dashboard	🗲 Back 🛛 Alerts Log					-	↓ Download Alert Logs
MONITORING							
Configuration	Events Log						
Logs						Search	12
(1)	View Alerts			Pomoto			
Restart	View Raw Log mp ⊺↓ Manage Log	Host 11	Request line	Address	Rule Id $^{+1}$	Message	Rule Message 🛛
ADDONS	29/Jut/2022:09:27:20 +0000	testphp.vulnweb.c om	POST /userinfo.php HTTP/1.1	10.10.171.23	941380	AngularJS client side template injection detected	Warning. Pattern match "{[*?}]" at ARGS:urname.
DLP	03/Aug/2022:09:26:19 +0000	testphp.vulnweb.c om	POST /userinfo.php HTTP/1.1	10.10.171.23	942370	Detects classic SQL injection probings 2/3	Warning. Pattern
© Help	03/Aug/2022:09:26:19 +0000	testphp.vulnweb.c om	POST /userinfo.php HTTP/1.1	10.10.171.23	942260	Detects basic SQL authentication bypass attempts 2/3	Warning. Pattern
•	03/Aug/2022:09:26:19 +0000	testphp.vulnweb.c om	POST /userinfo.php HTTP/1.1	10.10.171.23	942130	SQL Injection Attack: SQL Tautology Detected	Warning. Pattern
	03/Aug/2022:09:26:19 +0000	testphp.vulnweb.c om	POST /userinfo.php HTTP/1.1	10.10.171.23	942130	SQL Injection Attack: SQL Tautology Detected	Warning. Pattern





Click on any event line to see more details of the event

Modshield SB	× +					~ - 🗆 X
← → C	▲ Not secure 10.10.171.19:5000/fw_lo	og				🛛 🕒 Guest 🗄
AT.						
Ca Dashböerd						
Honistininii Je Configuration			Attack Details		×	
Lagr			Timestamp:	29/Jul/2022:	09:27:20 +0000	
(j) Firstart		Host	Transaction ID: Host: Attacker IP:	YuOn@PBerAuUnui testpl	BJIFbNwAAAEU hp.vulnweb.com 10.10.171.23	
Accession Inc. Court Batancer		testphp.vulnwel om	Rule ID: Description: AngularJS client side ten	nplate iniection detecte	941380 d	
				Add to blackli	st Close	
е нар						

Blacklist IP

To blacklist the IP that is shown in the event, simply click the respective row, in "Attack details" you can see the "Add to Blacklist"

62				
Carl Second				
and a second				
Q): Occurrent		⚠ Attack Details ×		
		Timestamp: 18/Au/2022/18/00/06/060254 +0530		
an Intel Conserve III III		Transaction ID: Vv4wzostL98nA14qotPD7wAAAEE Hest: 127001 Attacker IP: 12701 Rule ID: 920350		
		Description: Host header is a numeric IP address Add to blacklist Close Analyse logs		





Analyse Logs

To deeply analyse the event, you can simply click "Analyse logs" in the attack details of the respective event in the Alert Logs.

<u></u>					
(2) thethered					
Montpoint and					
Sector Sector					
: CO: Decento		Attack Details			
ADDITION S		Timestamo:	18/400/2022:18:00:06 060254 ±0530		
ta Lind Paterne III US		Transaction ID: Host: Attacker IP: Rule ID:	Yv4wzostL98nA14qotPD7wAAAEE 127.0.0.1 920350		
		Description: Host header is a numeri Add to blackli	c IP address		

After clicking the "Analyse Logs" you will be seeing the structured and categorized event log in a new tab

- transaction: {

 local_address: "10.10.176.207",
 local_port: 80,
 remote_address: "59.95.93.186",
 remote_port: 41658,
 time: "24/Aug/2022:13:04:39 +0000",
 transaction_id: "YwYh57XlQd4G7NlugfX0QAAAAFE"

• response: {

00058: (*) © body: "</DOCTYPE html> <html> <html <html> <html < 0.0.7); text-align: center; padding-top: 50px; } landing { position: relative; background-image: url('{{ url_for ('static', filename='img/landing_bg.jpg') }); background-size: cover; background-position: center; height: 100vh; }

 15vw;'> <img src=\"{{ url_for ('static', filename='img/landing_bg.jpg') }}'' style=</td>
 </html>", <hr/>

- 1.

```
protocol: "HTTP/1.1",
status: 200
```







Download Alert Logs

You can download "Alert Logs" simply clicking the "Download Alert Logs" button at the top right side of the page. You can choose to store it in any location locally

Modshield SB	× +							~ - 🗆 ×
← → C	A Not secure 10.10.171.19:5000/fw_lo	g						Guest :
AH.						≅ 3	÷	Administrator
Dashboard	← Back Alerts Log							✤ Download Alert Logs
MONITORING								
Configuration	Events Log							
Logs	Show 10 entries						Search	
() Restart	Timestamp ⊺∔	Host 🌐	Request line	Remote Address	Rule Id 💷	Message		Rule Message 👘
ADDONS	29/Jul/2022:09:27:20 +0000	testphp.vulnweb.c om	POST /userinfo.php HTTP/1.1	10.10.171.23	941380	AngularJS client side template injection detected		Warning. Pattern
E DLP	Showing 1 to 1 of 1 entries							Previous 1 Next
© Неф								

View Raw Logs

Modshield also provides an easy interface to view the associated raw logs. Select View Raw Logs from the Log Menu

Modshield Si	в × +						~ - ¤ ×
$\leftrightarrow \rightarrow c$	A Not secure 10.10.171.19:5000/fw_log						Guest :
Ā						⊠ 2 ⊕	Administrator
Dashboard MONITORING	← Back Alerts Log					l	✤ Download Alert Logs
الم Configuration	Events Log						
Logs	LOG MANAGEMENT tries View Alerts					Search	1:
() Restart	View Raw Log mp 1	Host 💠	Request line	Remote Address	Rule Id 🖽	Message	Rule Message
ADDONS	29/Jul/2022:09:27:20 +0000	testphp.vulnweb.c om	POST /userinfo.php HTTP/1.1	10.10.171.23	941380	AngularJS client side template injection detected	Warning. Pattern match "{{*?}}" at ARGS:urname.
DLP	03/Aug/2022:09:26:19 +0000	testphp.vulnweb.c om	POST /userinfo.php HTTP/1.1	10.10.171.23	942370	Detects classic SQL injection probings 2/3	Warning. Pattern
© Help	03/Aug/2022:09:26:19 +0000	testphp.vulnweb.c om	POST /userinfo.php HTTP/1.1	10.10.171.23	942260	Detects basic SQL authentication bypass attempts 2/3	Warning. Pattern
	03/Aug/2022:09:26:19 +0000	testphp.vulnweb.c om	POST /userinfo.php HTTP/1.1	10.10.171.23	942130	SQL Injection Attack: SQL Tautology Detected	Warning. Pattern
	03/Aug/2022:09:26:19 +0000	testphp.vulnweb.c om	POST /userinfo.php HTTP/1.1	10.10.171.23	942130	SQL Injection Attack: SQL Tautology Detected	Warning. Pattern





This lists all the log entries. The entries are in JSON format.

Modshield !	58 × +								~ - 🗆 ×
← → C	A Not secure 10.10.171.19:5000/log	mgmt							Guest :
AN I						-	S 4	•	Administrator 🕘
20 Dashboard	← Back Raw Log								
MONITORING	The current log size is 428.6 KB.	Displaying last 25 entries.							
Configuration	Raw Log								
Logs	{"transaction":{"time":"03/ {"transaction":{"time":"03/ {"transaction":{"time":"03/	ug/2022:09:26:19 +0000","transact: ug/2022:09:26:17 +0000","transact ug/2022:09:26:13 +0000","transact	ion_id":"Yuo-O@WmXdSq; ion_id":"Yuo-O@WmXdSq; ion id":"Yuo-NeWmXdSq;	ZyzAvytY4AAAAAc","rem ZyzAvytY3wAAAAE","rem ZyzAvytY3gAAAAA","rem	mote_address":"10.10. mote_address":"10.10. mote address":"10.10.	171.23","rem 171.23","rem 171.23","rem	ote_port": ote_port": ote_port":	61601,"loca 61601,"loca 61601,"loca	al_address":"10.1 al_address":"10.1 al_address":"10.1
Restart ADDONS	{"transaction":{"time":"03/ {"transaction":{"time":"03/ {"transaction":{"time":"03/	ug/2022:09:26:11 +0000","transact ug/2022:09:26:08 +0000","transact ug/2022:09:26:06 +0000","transact	ion_id":"Yuo-M@WmXdSq; ion_id":"Yuo-MOWmXdSq; ion_id":"Yuo-LuWmXdSq;	ZyzAvytY3QAAAAI", "rem ZyzAvytY3AAAABY", "rem ZyzAvytY2wAAABg", "rem	mote_address":"10.10.: mote_address":"10.10.: mote_address":"10.10.:	171.23","rem 171.23","rem 171.23","rem	ote_port" ote_port" ote_port"	61601,"loca 61601,"loca 61601,"loca	al_address":"10.: al_address":"10.: al_address":"10.:
Load Balancer	{"transaction":{"time":"03/ {"transaction":{"time":"03/ {"transaction":{"time":"03/	ug/2022:09:26:04 +0000","transact: ug/2022:09:26:01 +0000","transact: ug/2022:09:25:57 +0000","transact	ion_id":"Yuo-K@yjwrMX ion_id":"Yuo-KeyjwrMX ion_id":"Yuo-JeyjwrMX	3jNLF19sJQAAAEg","rem 3jNLF19sJAAAAEI","rem 3jNLF19sIwAAAEM","rem	mote_address":"10.10. mote_address":"10.10. mote_address":"10.10.	171.23","rem 171.23","rem 171.23","rem	ote_port" ote_port" ote_port"	61585,"loca 61585,"loca 61585,"loca	al_address":"10.1 al_address":"10.1 al_address":"10.1
E DLP	{ transaction :{ time : 03/ { "transaction":{ "time":"03/ { "transaction":{ "time":"03/ { "transaction":{ "time":"03/	ug/2022:09:25:39 +0000","transact ug/2022:09:25:33 +0000","transact ug/2022:09:25:30 +0000","transact	ion_id : Yuo-EeyyjwrMX: ion_id : Yuo-DeWmXdSq; ion_id : Yuo-CuWmXdSq; ion_id : Yuo-BébemXdSq;	3]NLF19S1gAAAEU", rem ZyzAvytY2gAAABM","rem ZyzAvytY2QAAABC","rem ZyzAvytY2AAAABC","rem	mote_address : 10.10. mote_address : 10.10. mote_address : 10.10. mote_address : 10.10.	171.23", "rem 171.23", "rem 171.23", "rem 171.23", "rem	ote_port" ote_port": ote_port":	61576, 1008 61572, "loca 61572, "loca 61572, "loca	al_address : 10. al_address":"10.1 al_address":"10.1 al_address":"10.1
(C) Help	<pre>{"transaction":{"time":"03/ {"transaction":{"time":"03/ {"transaction":{"time":"03/ </pre>	ug/2022:09:25:25 +0000","transacti ug/2022:09:25:23 +0000","transacti	ion_id":"Yuo-BeWmXdSq ion_id":"Yuo-A@yjwrMX	ZyzAvytY1wAAABI","rem 3jNLF19sIQAAAFQ","rem	mote_address":"10.10. mote_address":"10.10.	171.23","rem 171.23","rem	ote_port" ote_port" ote_port"	61572, "loca 61568, "loca	al_address":"10. al_address":"10.
•									

You can copy an entry that you are interested in, and beautify it using any tool

Modshield	a x +					~ - ¤ ×
$\leftrightarrow \rightarrow c$	▲ Not secure 10.10.171.19:5000/log_mgmt					Guest :
Ā		8	8		•	Administrator 🔋
Dashboard	Ce Back Raw Log					
	The current log size is 428.6 KB. Displaying last 25 entries.					
Configuration	Raw Log					
Logs () Restart ADDONS	<pre>["transaction":{"time":"03/Aug/2022:09:26:19 +0000","transaction_id":"Yuo-O@AmXdSq2yzAvytY4AAAAAC", "remote_address":"10.10.171.; {"transaction":{"time":"03/Aug/2022:09:26:17 +0000","transaction_id":"Yuo-O@AmXdSq2yzAvytY3AAAAAC", "remote_address":"10.10.171.; {"transaction":{"time":"03/Aug/2022:09:26:13 +0000","transaction_id":"Yuo-NeAmXdSq2yzAvytY3AAAAA","remote_address":"10.10.171.; {"transaction":{"time":"03/Aug/2022:09:26:11 +0000","transaction_id":"Yuo-NeAmXdSq2yzAvytY3AAAAA","remote_address":"10.10.171.; {"transaction":{"time":"03/Aug/2022:09:26:08 +0000","transaction_id":"Yuo-NeAmXdSq2yzAvytY3AAAAB","remote_address":"10.10.171.; {"transaction":{"time":"03/Aug/2022:09:26:08 +0000","transaction_id":"Yuo-NeAmXdSq2yzAvytY3AAAAB","remote_address":"10.10.171.; {"transaction":{"time":"03/Aug/2022:09:26:08 +0000","transaction_id":"Yuo-NeAmXdSq2yzAvytY3AAAAB","remote_address":"10.10.171.; {"transaction":{"time":"03/Aug/2022:09:26:08 +0000","transaction_id":"Yuo-UAMXdSq2yzAvytY3AAAAB","remote_address":"10.10.171.; {"transaction":{"time":"03/Aug/2022:09:26:08 +0000","transaction_id":"Yuo-UAMXdSq2yzAvytY3AAAAB","remote_address":"10.10.171.; {"transaction":{"time":"03/Aug/2022:09:26:08 +0000","transaction_id":"Yuo-UAMXdSq2yzAvytY3AAAB","remote_address":"10.10.171.; {"transaction":{"time":"03/Aug/2022:09:26:08 +0000","transaction_id":"Yuo-UAMXdSq2yZAvytY3AAAB","remote_address":"10.10.171.; {"transaction":{"time":"03/Aug/2022:09:26:08 +0000","transaction_id":"Yuo-UAMXdSq2yZAvytY3AAAB","remote_address":"10.10.171.; {"transaction":{"time":"03/Aug/2022:09:26:08 +0000","transaction_id":"Yuo-UAMXdSq2yZAvytY3AAAB","remote_address":"10.10.171.; {"transaction":{"time":"03/Aug/2022:09:26:08 +0000","transaction_id":"Yuo-UAMXdSq2yZAvytY3AAAB","remote_address":"10.10.171.; {"transaction":{"time":"03/Aug/2022:09:26:08 +0000","transaction_id":"Yuo-UAMXdSq2yZAvytY3AAAB","remote_address":"10.10.171.; {"transaction":{"time":"03/Aug/2022:09:26:08 +0000","transaction_id":"Yuo-UAMXdSq2yZAvytY3AAAB","timete_address":"10.10.171.; {"tra</pre>	23","rem 23","rem 23","rem 23","rem 23","rem 23","rem	ote_por ote_por ote_por ote_por ote_por ote_por	t":6160 t":6160 t":6160 t":6160 t":6160 t":6160	01,"local_ 01,"local_ 01,"local_ 01,"local_ 01,"local_ 01,"local_ 01,"local_	address":"10. address":"10. address":"10. address":"10. address":"10. address":"10.
Load Balancer	<pre>("transaction": ("time":"03/Aug/2022:09:26:04 +0000","transaction_id":"Yuo-K@yjerMX3jHLF9sJAAAEE","remote_address":"10.10.171. ("transaction": ("time":"03/Aug/2022:09:26:01 +0000","transaction_id":"Yuo-KeyjerMX3jHLF19sJAAAEET", "remote_address":"10.10.171. ("transaction": ("time":"03/Aug/2022:09:25:57 40000","transaction_id":"Yuo-VeyjerMX3jHLF19sJAAAEET","remote_address "10.10.171.</pre>	23","rem 23","rem 23","rem	ote_por ote_por ote_por	t":6158 t":6158 t":6158	85,"local_ 85,"local_ 85,"local_	_address":"10.: _address":"10.: _address":"10.:
DLP	<pre>{"transaction":{"time":"63/Aug/2022:09:25:39 +0000","transaction_id":"Yuo-E@yim+XX:3NLF19sTgAAEU","remote_address":"10.10.171.; ("transaction":{"time":"63/Aug/2022:09:25:33 +0000","transaction_id":"Yuo-DeAmAdSq2y2AvytY2gAAABM","remote_address":"10.10.171.; ("transaction":{"time":"63/Aug/2022:09:25:32 +0000","transaction_id":"Yuo-CAMAdSq2y2AvytY2gAAABC","remote_address":"10.10.171.; ("transaction":{"time":"63/Aug/2022:09:25:27 +0000","transaction_id":"Yuo-B@AmAdSq2y2AvytY2gAAABC","remote_address":"10.10.171.;</pre>	23","rem 23","rem 23","rem 23","rem	ote_por ote_por ote_por ote_por	t":6157 t":6157 t":6157 t":6157	76,"local_ 72,"local_ 72,"local_ 72,"local_ 72,"local_	address": "10.: address": "10.: address": "10.: address": "10.:
e Help	{"transaction";{"time":"%3/Aug/2022:09:25:25 +0000","transaction_id":"Yuo-BeAmAdSq2y2AvytYtAMAABI","remote_address":"10.10.171.7 {"transaction";{"time":"%3/Aug/2022:09:25:23 +0000","transaction_id":"Yuo-A@yjwrXX3HLF19sIQAAAFQ","remote_address":"10.10.171.7	23","rem 23","rem	ote_por ote_por	t":6157 t":6156	2,"local_ 8,"local_	_address":"10.: _address":"10.:



I use beautifier.io to render the log entry in a readable JSON format. When you forward logs to an external listener, this is the format that you will be parsing



Download Raw Logs

Log files need to be managed, archived or transferred. This can be done using the Manage Log Option

Modshield S	8 × +				~ - ¤ ×
$\leftrightarrow \rightarrow G$	▲ Not secure 10.10.171.19:5000/manage_log				Guest :
AH I				■ 2 +	Administrator
20 Dashboard	Manage Log			Clear Logs	Download Logs
MONITORING	Configure FTP Service			Ma	we to FTP Save Changes
Configuration		IP Address			
Logs	log management View Alerts	Username			
() Restart	View Raw Log	Password			
ADDONS		Secure FTP	Disabled		
Load Balancer		Directory			
EL DLP					
() Неф	Configure Log Forwarding Service				Save Changes
		Log Forwarding Service	Disabled		
	~~ <u>~</u>				

MODSHIELD





The Download Log button allows you to download a copy of the log file, locally

Modshield SE	* × +				~ - O ×
← → C	▲ Not secure 10.10.171.19:5000/manage_log				Guest :
る語				■ 0 +	Administrator
Dashboard	Manage Log			Clear Logs	Download Logs
	Configure FTP Service			M	ove to FTP Save Changes
Configuration		IP Address			
Logs		Username			
() Restart		Password			
		Secure FTP	Disabled		
Load Balancer		Directory			
(2) Неф	Configure Log Forwarding Service				Save Changes
	11	Log Forwarding Service	Disabled		
	1 - 1 ()				

You can choose to store it in any location locally

Save As		×
\leftarrow \rightarrow \checkmark \uparrow \blacksquare > This PC >	・ CSearch This PC	Q
Organize 🔻	10 T	• ?
Add Domain_V1 Apr 2020 Evolution Aus SurfaceAl		^
ConeDrive Desktop		
This PC 3 D Objects Desktop		~
File name: ModShieldSB.log		~
Save as type: Text Document (*.log)		~
∧ Hide Folders	Save	Cancel .::





Transfer Logs using FTP

You can also transfer the log files using FTP

Modshield Si	8 × +				~ - 🗆 ×
$\leftrightarrow \rightarrow c$	▲ Not secure 10.10.171.19:5000/manage_log				Guest :
AH .				≊ £ ∲ /	Administrator
Dashboard	Manage Log			Clear Logs	Download Logs
	Configure FTP Service			Move	e to FTP Save Changes
Configuration		IP Address			
Logs		Username			
() Restart	•	Password			
		Secure FTP	Disabled		
Load Balancer		Directory			
DLP					
© Hetp	Configure Log Forwarding Service				Save Changes
\bullet	D ^o	Log Forwarding Service	Disabled		

Simply configure the FTP details and the directory to which the log files are to be transferred. You can enable secure FTP if it is allowed for your transfer

Modshield Si	18 × +				~ - ¤ ×
$\leftrightarrow \rightarrow \ G$	▲ Not secure 10.10.171.19:5000/manage_log				Guest :
ĀĦ				≡ 2 + 4	Administrator 😐
Dashboard	Manage Log			Clear Logs	Download Logs
MONITORING	Configure FTP Service			Move to	o FTP Save Changes
Configuration		IP Address	12.12.12.12		
Logs		Username	tftp		
() Restart		Password	****		
ADDONS		Secure FTP	Disabled		
Load Balancer		Directory	todays_logs		
E DIP					
(C) Help	Configure Log Forwarding Service				Save Changes
•	1 12	Log Forwarding Service	Disabled		
	····				



Once configured, click on "Move to FTP" to move the log file. Once moved, the log files will be cleared in the firewall and the dashboards refreshed

Modshield Si	8 × +				~ - ¤ ×
← → C	A Not secure 10.10.171.19:5000/manage_log				Guest :
A				■ 2 +	Administrator
Dashboard	Manage Log			Clear Logs	Download Logs
	Configure FTP Service				Nove to FTP Save Changes
Configuration		IP Address	12.12.12.12		
Logs		Username	tftp		
() Restart		Password	••••		
		Secure FTP	Disabled		
Load Balancer		Directory	todays_logs		
DLP					
© Help	Configure Log Forwarding Service				Save Changes
	11	Log Forwarding Service	Disabled		
	····				

Log Forwarding

You can enable real time log forwarding to an external listener service

Modshield SB	× +				~ - O ×
← → C	Not secure 10.10.171.19:5000/manage_log				Guest :
AN .				S & + +	Administrator
Dashboard	Manage Log			Clear Logs	Download Logs
MONITORING	Configure FTP Service			Move to	FTP Save Changes
Configuration		IP Address	12.12.12.12		
Logs		Username	tftp		
() Restart		Password	••••		
ADDONS		Secure FTP	Disabled		
Load Balancer		Directory	todays_logs		
(c) Help	Configure Log Forwarding Service				Save Changes
•	1	Log Forwarding Service	Disabled		

MODSHIELD^{SB}





Enable this service to forward every log entry as it is written to the log file

Modshield SE	x +				~ - 🗆 ×
← → C	▲ Not secure 10.10.171.19:5000/manage_log				Guest :
AH .				≥ C +	Administrator
Dashboard	Manage Log			Clear Logs	Download Logs
	Configure FTP Service				Nove to FTP Save Changes
Configuration		IP Address	12.12.12.12		
Logs		Username	tftp		
() Restart		Password	••••		
		Secure FTP	Disabled		
Load Balancer		Directory	todays_logs		
EI DLP					
(2) Help	Configure Log Forwarding Service				Save Changes
	1 12	Log Forwarding Service	Disabled		
			Enabled Disabled		

Enter the IP address and the port details of the listener and Save Changes

Modshield Si	8 × +				~ - 0 X
← → C	▲ Not secure 10.10.171.19:5000/manage_log				Guest :
AN .				S & + +	Administrator (3)
Dashboard	Manage Log			Clear Logs Dov	wnload Logs
MONITORING	Configure FTP Service			Move to FTP	Save Changes
Configuration		IP Address	12.12.12.12		
		Username	tftp		
() Restart		Password			
		Secure FTP	Disabled		
Load Balancer		Directory	todays_logs		
EL DLP					
(2) Неф	Configure Log Forwarding Service				Save Changes
•	a Bach	Log Forwarding Service	Enabled		
		Destination	192.168.1.200:4455		

The forwarded messages will be in the same JSON format as in the raw logs.





Update Modshield

Video Link: <u>https://youtu.be/OpNaGKcRpHI</u>

Modshield is constantly kept current through updates that are published regularly

To update Modshield, scroll down to the update section in Firewall configuration

Modshield SB	× +						~ - O ×
← → C	A Not secure 10.10.171.19:5000/mg_firewall						Guest :
AN .				-	C 4	⊨	Administrator
2 Dashboard	Manage Firewall						
	Configure Modshield Service						Save Changes
Configuration	CONFIGURATION SSL Certificate	Paranoia Level	Paranoia Level 2				
Logs	Domain Configuration						
() Restart	Access Filtering	Select Engine Mode	Detection + Blocking				
	RULES MANAGEMENT	Request Limit (bytes)	524228				
Load Balancer	Custom Ruleset	File Upload Scanner	Disabled				
E DI P	~	Response Processing	Enabled				
		Log Policy	Log blocked threats				
(C) Help		IP Reputation Filter	Enabled				
		DoS Protection	Disabled				

Threat intelligence, rules, software and the Geo IP data updates are made available

Modshield SB	× +					~ - O	×
← → C ▲ Not secu	ure 10.10.171.19:5000/mg_firewall					Guest	(
		Status: TRIAL - ACTIVATED Your currrent license expires in 6 days.	8	C	•	Administrator 🔋	
Custon	mization					Save Changes	
	\$	Error Page Choose File No file chosen					
Update	te, Backup/Restore						
	1 .	Download update: Update Modshield Manage Modshield Configuration: Import Configuration Export Configuration					
Import	t Logs						
	1.	1 Import from file					





Update License

You can also update any changes in your license information using this screen

Modshield SB	× +						~ - 🗆 ×
← → C ▲	Not secure 10.10.171.19:5000/mg_firewall						Guest :
		DoS Protection		s 3		٠	Administrator
	Configure SafelP						Save Changes
		Domain	testphp.vulnweb.com				
		Allowed IP					
	Licensing						Save Changes
	_	License Key	KEMLQ-BJYEW-CQUYR-ISXDM				
		Status: TRIAL - ACTIVATED Your currrent license expires in (6 days.				
	Customization						Save Changes
	\$	Error Page	Choose File No file chosen				•

Update Threat Intelligence Feeds

Threat Intel provides Modshield with information to identify bots, crawlers, bad IPs and so on

Modshield SB	× +					~ - • ×
← → C ▲	Not secure 10.10.171.19:5000/mg_firewall					Guest 🔅
		Status: TRIAL - ACTIVATED Your currrent license expires in 6 days.	-	Ø	•	Administrator (3)
	Customization					Save Changes
	\$ °	Error Page Choose File No file chosen				
	Update, Backup/Restore					
	1.	Download update: Lupdate Modshield Lupdate Threat Intel Manage Modshield Configuration: Import Configuration Lupdate Threat Intel Export Configuration				
	Import Logs					
	1	Import from file				





Modshield Updates

Modshield upgrades help us push rules and software updates to all instances

Modshield SB	× +						~ - a ×
← → C	A Not secure 10.10.171.19:5000/mg_firewall						Guest 📋
		Status: TRIAL - ACTIVATED Your currrent license expires in 6 days.	8	ø	÷	•	Administrator 📳
	Customization						Save Changes
	\$ °	Error Page Choose File No file chosen					
	Update, Backup/Restore						
	<u>.</u>	Download update: LUpdate Modshield LUpdate Threat Intel Manage Modshield Configuration: Import Configuration Lupdate Threat Intel					
		L Import from file					





Import / Export Configuration

To back up the firewall configuration, you can export the configuration and store it locally

Modshield SB	× +					~ - 0 ×
← → C	Not secure 10.10.171.19:5000/mg_firewall					Guest 🔅
		Status: TRIAL - ACTIVATED Your currrent license expires in 6 days.	ø	÷	▲	Administrator 📳
	Customization					Save Changes
	\$	Error Page Choose File No file chosen				
	Update, Backup/Restore					
	1	Download update:				
						_
	Import Logs					
	1	1 Import from file				

You can also use that to import the configuration into another firewall instance

Modshield SB	× +						~ - ¤ ×
← → C ▲	Not secure 10.10.171.19:5000/mg_firewall						Guest 🔅
		Status: TRIAL - ACTIVATED Your currrent license expires in 6 days.	8	ø	÷	•	Administrator 📳
	Customization						Save Changes
	\$ °	Error Page Choose File No file chosen					
	Update, Backup/Restore						
	1	Download update: Lupdate Modshield Lupdate Threat Intel Manage Modshield Configuration: Luport Configuration					
	Import Logs						
	1	1 Import from file					^


This is very useful if you are managing multiple firewalls and would like to replicate the settings. This also allows you to import custom rules, DLP settings etc. from another firewall

💿 Open				×
\leftarrow \rightarrow \checkmark \uparrow \square \ll Win	dows (C:) > Config backup >	~ ∂	Search Config back	o , qu
Organize 🔻 New folder	r			- 🔳 😮
🗄 Documents \land	Name	D	ate modified	Туре
🕂 Downloads	🔚 modshield_config.zip	04	1-05-2020 16:00	WinRAR ZIP arcl
b Music				
Pictures				
Videos				
🟪 Windows (C:)				
HP_RECOVERY (
HP_TOOLS (E:)				
💣 Network				
DESKTOP-GG7A(🗡	<			>
File na	me: modshield_config.zip	~	WinRAR ZIP archive	e (*.zip) 🗸 🗸
	L		Open 🔽	Cancel

We encourage you to keep your firewall instance updated regularly using these options

Dashboard - ModShield SB × +							- 0	×
← → C ▲ Not secure 3.34.14.172:5000/mg_firewall			☆	G	0	4	J Paused) :
••••	Allowed IPs	Enter Destination (IP:Port)						ľ
								h
Licensing						Save	Changes	
	License Key	HIHBI-MEV07-7N7IC-MENWS						
	Licenseriey							
<u>∠</u> =	Status: TRIAL - ACTIVATED							
	rour current license expires in 24 days.							
								- -
Update Modshield								
	L Upgrade Modshield							
		IP-Geography definitions						
	Manage ModShield Config	ration						
		ation 1 Export Configuration						
								Ţ.

MODSHIELD^{SB}





References

Certain definitions from OWASP, SANS and Wikipedia have been referred to in the creation of this document

