



Virtual Firewall Appliance

User Guide

September 7, 2018

Copyright 2018 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100



Table of Contents

VMware and Hyper-V Configuration.....	4
Import and Register your WAF Appliance.....	4
Set Up the Appliance using the CLI.....	6
Reboot may be required.....	7
Verify Registration.....	7
WAF registration parameters.....	8
Amazon EC2 Configuration.....	9
Launch New EC2 Instance.....	9
Add Your WAF AMI to the Load Balancer	11
Microsoft Azure Configuration	14
Deploy WAF on Azure	14
Google Cloud Configuration	17
Deploy WAF on Google Cloud Platform	17
Docker Configuration	20
CLI Reference	21
Commands	21
Variables.....	23
Contact Support.....	24

VMware and Hyper-V Configuration

Follow the steps below to deploy your WAF firewall cluster in VMware (vCenter) or Microsoft Hyper-V and configure your DNS. You'll need to funnel traffic through the WAF cluster by changing your DNS.

Once you complete these steps, we'll start monitoring your web application for security violations. Also your WAF cluster will start making outbound connections to the Qualys Cloud Platform for regular health checks - these confirm the cluster is properly configured and has the latest software.

Tell me the steps

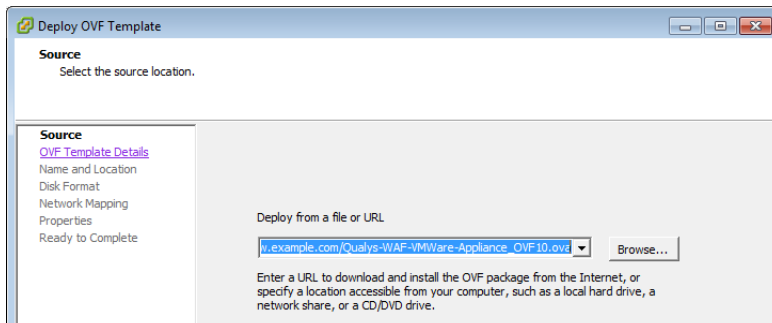
- 1) Download the OVA image (VMware) or the VHD image (Hyper-V). You'll get the image when you add a new WAF appliance (go to WAF Appliances > WAF Clusters, click the New WAF Appliance button).
- 2) Import the image in your virtualization platform. The OVA image supports VMware for production (and can be used in VirtualBox for test purposes only), while the VHD image supports Microsoft Hyper-V.
- 3) Set up the virtual appliance using the CLI (Command Line Interface).
- 4) Verify the registration of the appliance.
- 5) Test availability of your web application through Qualys WAF. Once confirmed, you'll need to alias DNS entries to direct traffic at your origin infrastructure.

Import and Register your WAF Appliance

Using vCenter

Start your VMware Client.

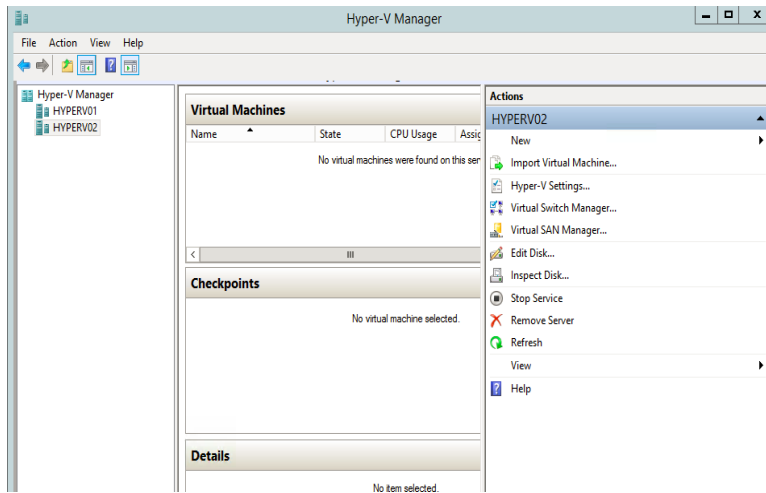
Choose "Deploy OVA File". This starts the OVA Template wizard. Browse to the downloaded OVA and select it (or enter the URL where the OVA can be downloaded).



Using Hyper-V

Start your Hyper-V Manager.

Select New > Virtual Machine... and using the “New Virtual Machine Wizard” create a new virtual machine.



Good to know

Hyper-V appliance currently does not support static network configuration through the CLI. You will need to setup an external DHCP configuration, and configure it to provide a permanent IP address to the VM's mac-address. Bear this in mind especially if you're using a virtual switch for WAF connectivity, on Hyper-V Manager. To monitor your network configuration through CLI, you can use "ifconfig", "show network", "network [help]", and "routes [help]" commands.

Step through the wizard

We provide a default name for your WAF instance, and you can change it. Select disk format and mapping settings appropriate for your environment. Do not set WAF-specific properties in the wizard as they are deprecated and will be removed in a future release. You will set properties using the CLI. See [Set Up the Appliance using the CLI](#)

Set Up the Appliance using the CLI

Log in as “waf-user” via SSH or System Console

The first login forces you to change your password.

```
$ ssh waf-user@10.1.1.5
You are required to change your password immediately (root
enforced)
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user waf-user.
New password: C-om34EhbTz.6aiMU4C
Retype new password: C-om34EhbTz.6aiMU4C
passwd: all authentication tokens updated successfully.

Connection to 10.1.1.5 closed.
```

Configuration

Set the required properties: waf_service_url (URL of Qualys Cloud Platform hosting your account) and registration_code. See [WAF registration parameters](#). More properties may be required depending on your networking environment. See [CLI Reference](#) for details.

```
$ ssh waf-user@10.1.1.5

qualys waf # help
Commands (type help <command>):
=====
deregister help passwd save show status viewlog diag ifconfig
reboot set shutdown sysinfo waf exit network routes setup ssh
unset

qualys waf # set
Syntax: set KEY=VALUE
Valid keys:
    waf_service_url
    proxy_url
    sem_syslog_addr
    registration_code
    waf_ssl_passphrase

qualys waf # set waf_service_url=https://rns.qualys.com
qualys waf # set registration_code=A30BC162-785A-4BAF-A5D5-
1A2DE9C6DA3A
qualys waf # save
Saved Successfully
```

Reboot may be required

...if you are changing the token (e.g. re-registration).

```
qualys waf # reboot
Are you sure you want to reboot? <y/N> y
Rebooting

Broadcast message from waf-user@dhcp-10-1-1-5
(/dev/pts/0) at 18:05 ...

The system is going down for reboot NOW!
Connection to 10.1.1.5 closed.
```

Verify Registration

You can do this using the CLI as shown below, or the WAF user interface (go to WAF Appliances > WAF Clusters).

```
qualys waf # status
Checking status.... Done.
Connectivity to Qualys: OK
Registration status: OK
Sensor Id: 2b9af5aa-f99e-45bf-86dd-3d45a4d6b3f7
Registration Code: 3F159371-6188-4B7C-8C6D-48E764ADF00D
qualys waf # quit

Connection to 10.1.1.5 closed.
```

Note: When you check the appliance status, “Connectivity to Qualys” may show OK even if you do not set the WAF_SERVICE_URL. This is because WAF_SERVICE_URL takes the default value `https://rms.qualys.com:443/` when not explicitly set to a custom value.

That’s it! You’ve configured your WAF virtual appliance. Once you’re done we’ll start a distributed network of sensors for your WAF cluster. Also your WAF cluster will start making outbound connections to the Qualys Cloud Platform.

WAF registration parameters

While registering a WAF appliance, you need to provide WAF registration code and other properties as appropriate using the variables below:

Variable	Description												
WAF_SERVICE_URL	<p>(Required) The URL of the Qualys Cloud Platform hosting your Qualys account. Supported platform URLs are:</p> <table> <tr> <td>US Platform 1</td><td>https://rns.qualys.com</td></tr> <tr> <td>US Platform 2</td><td>https://rns.qg2.apps.qualys.com</td></tr> <tr> <td>US Platform 3</td><td>https://rns.qg3.apps.qualys.com</td></tr> <tr> <td>EU Platform 1</td><td>https://rns.qualys.eu</td></tr> <tr> <td>EU Platform 2</td><td>https://rns.qg2.apps.qualys.eu</td></tr> <tr> <td>India Platform 1</td><td>https://rns.qg1.apps.qualys.in</td></tr> </table> <p>Note: When you check the appliance status, "Connectivity to Qualys" may show OK even if you do not set the WAF_SERVICE_URL. This is because WAF_SERVICE_URL takes the default value https://rns.qualys.com:443/ when not explicitly set to a custom value.</p>	US Platform 1	https://rns.qualys.com	US Platform 2	https://rns.qg2.apps.qualys.com	US Platform 3	https://rns.qg3.apps.qualys.com	EU Platform 1	https://rns.qualys.eu	EU Platform 2	https://rns.qg2.apps.qualys.eu	India Platform 1	https://rns.qg1.apps.qualys.in
US Platform 1	https://rns.qualys.com												
US Platform 2	https://rns.qg2.apps.qualys.com												
US Platform 3	https://rns.qg3.apps.qualys.com												
EU Platform 1	https://rns.qualys.eu												
EU Platform 2	https://rns.qg2.apps.qualys.eu												
India Platform 1	https://rns.qg1.apps.qualys.in												
REGISTRATION_CODE	<p>(Required) Enter the WAF registration code in this format: REGISTRATION_CODE=your_code. You can find this code by going to the WAF clusters list (WAF Appliances > WAF Clusters).</p>												
PROXY_URL	<p>(Required if a proxy is required for the WAF cluster to access the Qualys Cloud Platform) If the WAF needs to connect to the Qualys Cloud Platform through an HTTP proxy, please input the URL of the proxy. Enter the proxy URL in this format: PROXY_URL=proxy_url</p>												
WAF_SSL_PASSPHRASE	<p>(Required if the appliance protects a site communicating over SSL) If your web application's primary or secondary base URL uses the HTTPS protocol, the Qualys Cloud Platform portal protects the private key by encrypting it with a 64 byte dedicated passphrase. This way, it's not accessible in clear on the Qualys Platform. This WAF_SSL_PASSPHRASE needs to be set on the appliance, for decrypting the key. Enter the passphrase in this format: WAF_SSL_PASSPHRASE=passphrase</p>												

Amazon EC2 Configuration

Follow the steps below to deploy your WAF firewall cluster in Amazon EC2 and configure your DNS. You'll need to funnel traffic through the WAF cluster by changing your DNS.

Once you complete these steps, we'll start monitoring your web application for security violations. Also your WAF cluster will start making outbound connections to the Qualys Cloud Platform for regular health checks - these confirm the cluster is properly configured and has the latest software.

Launch New EC2 Instance

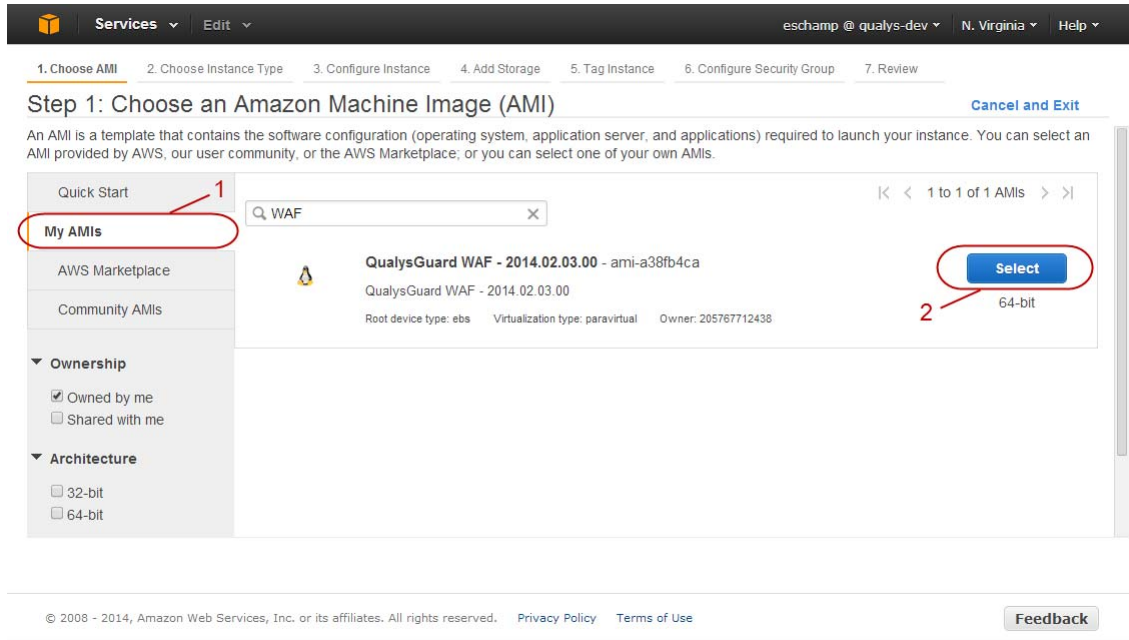
1) Go to your Amazon EC2 Dashboard and launch an instance

The screenshot displays the Amazon EC2 console interface. On the left, a navigation sidebar lists various services including EC2 Dashboard, INSTANCES, IMAGES, ELASTIC BLOCK STORE, and NETWORK & SECURITY. The main content area is titled 'Resources' and shows a summary of EC2 resources in the US East (N. Virginia) region, including 3 Running Instances, 84 Volumes, 11 Key Pairs, 0 Placement Groups, 7 Elastic IPs, 37 Snapshots, 0 Load Balancers, and 17 Security Groups. Below this summary, a 'Create Instance' section is visible, featuring a blue 'Launch Instance' button that is circled in red. To the right of the main content, there are sections for 'Account Attributes', 'Additional Information' (including links to documentation and forums), and 'Popular AMIs on AWS Marketplace'. At the bottom of the console, a 'Service Health' section indicates that the US East (N. Virginia) service is operating normally. The footer contains copyright information and links to the Privacy Policy and Terms of Use.

2) Choose the WAF AMI

Click My AMIs (1) and then select the QualysGuard WAF AMI (2).

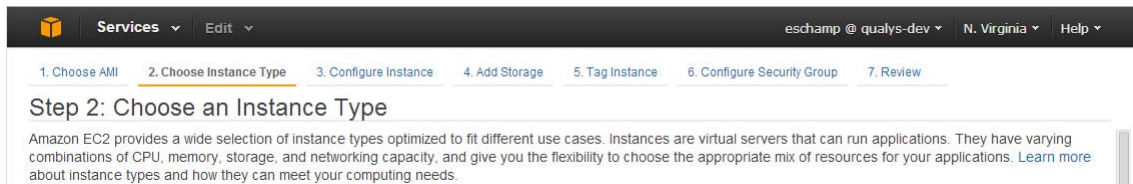
Tip Use the search box to find this quickly. Just enter “WAF” and click Enter.



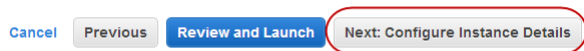
Don't see the WAF AMI? Please contact your Technical Account Manager or our Support Team for assistance.

3) Choose Instance Type

You'll choose from a wide variety of instance types.



Select an instance type and then click “Next: Configure Instance Details”.



4) Configuration

Open Advanced Details. In the User Data field, enter your WAF registration code and other properties as appropriate. See [WAF registration parameters](#).

5) Additional steps (optional)

You might want to add storage, tag the instance and configure security groups.

6) Click Review and Launch

Be sure to wait until the WAF AMI status is green (this means it's running). Then you're ready to add the AMI instance to the EC2 load balancer (see the next section).

Add Your WAF AMI to the Load Balancer

1) Create an HTTP Load Balancer Instance

Create a New Load Balancer Cancel

DEFINE LOAD BALANCER CONFIGURE HEALTH CHECK ADD EC2 INSTANCES REVIEW

This wizard will walk you through setting up a new load balancer. Begin by giving your new load balancer a unique name so that you can identify it from other load balancers you might create. You will also need to configure ports and protocols for your load balancer. Traffic from your clients can be routed from any load balancer port to any port on your EC2 instances. By default, we've configured your load balancer with a standard web server on port 80.

Load Balancer Name:

Create LB inside:

Create an internal load balancer: ☐ [\(what's this?\)](#)

Listener Configuration:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port	Actions
HTTP	80	HTTP	80	Remove
<input type="text" value="HTTP"/>	<input type="text"/>	<input type="text" value="HTTP"/>	<input type="text"/>	Save

[Continue](#)

2) Set up your Health Checks

Choose the TCP Ping Protocol option. Later, when your web application is online, you can choose a URL for a comprehensive health check.

Create a New Load Balancer

Cancel

DEFINE LOAD BALANCER

CONFIGURE HEALTH CHECK

ADD EC2 INSTANCES

REVIEW

Your load balancer will automatically perform health checks on your EC2 instances and only route traffic to instances that pass the health check. If an instance fails the health check, it is automatically removed from the load balancer. Customize the health check to meet your specific needs.

Configuration Options:

Ping Protocol: TCP

Ping Port: 80

Advanced Options:

Response Timeout: 5 Seconds
Time to wait when receiving a response from the health check (2 sec - 60 sec).

Health Check Interval: 0.5 Minutes
Amount of time between health checks (0.1 min - 5 min)

Unhealthy Threshold: 2 3 4 5 6 7 8 9 10
Number of consecutive health check failures before declaring an EC2 instance unhealthy.

Healthy Threshold: 2 3 4 5 6 7 8 9 10
Number of consecutive health check successes before declaring an EC2 instance healthy.

< Back

Continue >

3) Add Your WAF Instance in the Cluster

Click the “Select” check box beside your WAF instance to add it to the load balancer. Your load balancer is now created and will soon be able to handle requests.

Create a New Load Balancer

Cancel

DEFINE LOAD BALANCER

CONFIGURE HEALTH CHECK

ADD EC2 INSTANCES

REVIEW

The table below lists all your running EC2 Instances that are not already behind another load balancer or part of an auto-scaling capacity group. Check the boxes in the Select column to add those instances to this load balancer.

Manually Add Instances to Load Balancer:

Select	Instance	Name	State	Security Groups	Availability Zone
<input type="checkbox"/>	i-0ee4fd43	DRUPAL	running	quicklaunch-1	eu-west-1b
<input checked="" type="checkbox"/>	i-2ce6ff61	WAF	running	quicklaunch-1	eu-west-1b

select all

select none

Availability Zone Distribution:

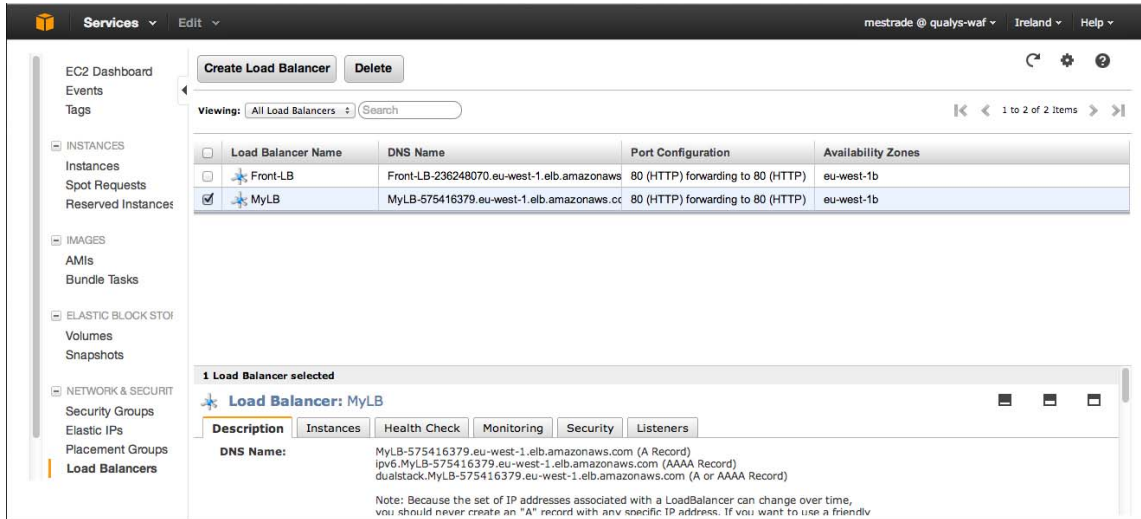
1 instances in eu-west-1b

< Back

Continue >

4) Redirect Your Traffic to the Load Balancer Hostname

Test the availability of your web application through the load balancer. Once confirmed, you'll need to alias your DNS entries to the Amazon EC2 load balancer you just created.



The screenshot shows the AWS Management Console interface for Amazon EC2 Load Balancers. The left sidebar contains navigation links for EC2 Dashboard, Events, Tags, INSTANCES (Instances, Spot Requests, Reserved Instances), IMAGES (AMIs, Bundle Tasks), ELASTIC BLOCK STORAGE (Volumes, Snapshots), and NETWORK & SECURITY (Security Groups, Elastic IPs, Placement Groups, Load Balancers). The main content area displays a table of Load Balancers with columns: Load Balancer Name, DNS Name, Port Configuration, and Availability Zones. Two load balancers are listed: 'Front-LB' and 'MyLB'. 'MyLB' is selected, and its details are shown in the 'Description' tab. The details include the DNS Name, a list of associated IP addresses (A, AAAA, and dualstack records), and a note about IP address changes over time.

Load Balancer Name	DNS Name	Port Configuration	Availability Zones
Front-LB	Front-LB-236248070.eu-west-1.elb.amazonaws.com	80 (HTTP) forwarding to 80 (HTTP)	eu-west-1b
MyLB	MyLB-575416379.eu-west-1.elb.amazonaws.com	80 (HTTP) forwarding to 80 (HTTP)	eu-west-1b

1 Load Balancer selected

Load Balancer: MyLB

Description | Instances | Health Check | Monitoring | Security | Listeners

DNS Name: MyLB-575416379.eu-west-1.elb.amazonaws.com (A Record)
ipv6.MyLB-575416379.eu-west-1.elb.amazonaws.com (AAAA Record)
dualstack.MyLB-575416379.eu-west-1.elb.amazonaws.com (A or AAAA Record)

Note: Because the set of IP addresses associated with a LoadBalancer can change over time, you should never create an "A" record with any specific IP address. If you want to use a friendly

That's it! You've configured your WAF virtual appliance. Once you're done we'll start a distributed network of sensors for your WAF cluster. Also your WAF cluster will start making outbound connections to the Qualys Cloud Platform (HTTPS over TCP-443).

Microsoft Azure Configuration

Follow the steps below to deploy your WAF firewall on Microsoft Azure.

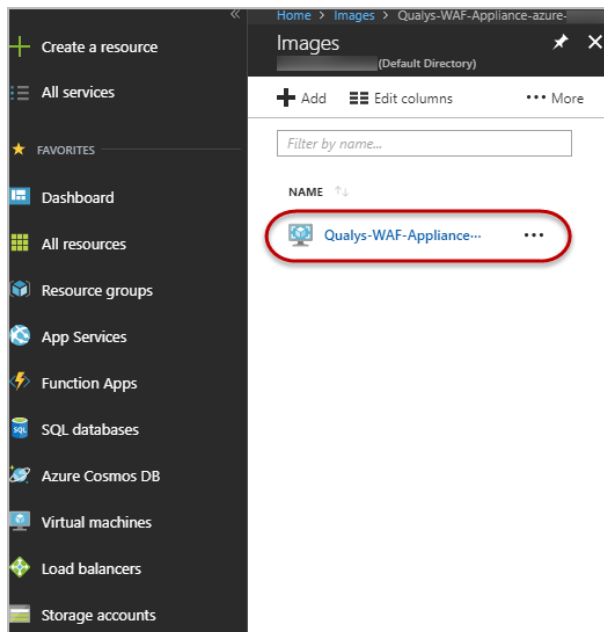
Once you complete these steps, we'll start monitoring your web application for security violations. Also your WAF appliance will start making outbound connections to the Qualys Cloud Platform for regular health checks - these confirm the appliance is properly configured and has the latest software.

Deploy WAF on Azure

1) Go to your Azure Dashboard and under Images find the Qualys WAF image.

Click All services, and then click Images. Search for the WAF image.

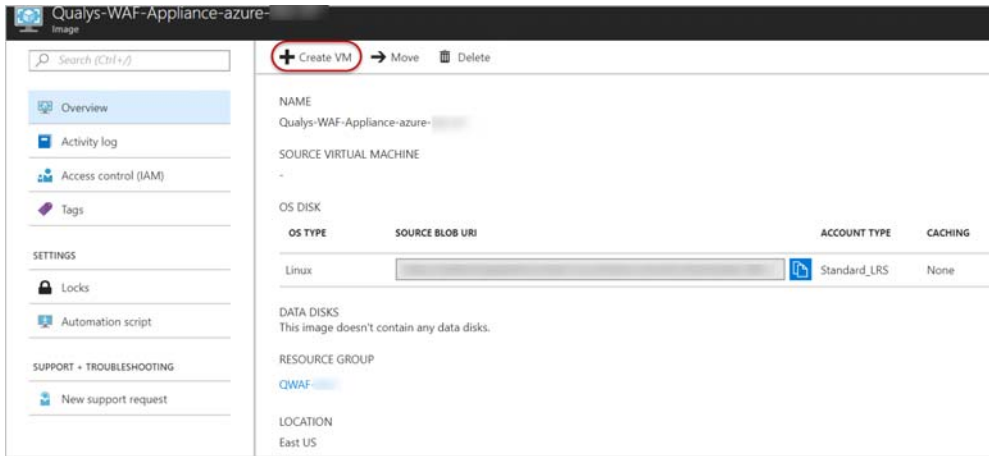
Tip Use the search box to find this quickly. Just enter "WAF" and click Enter.



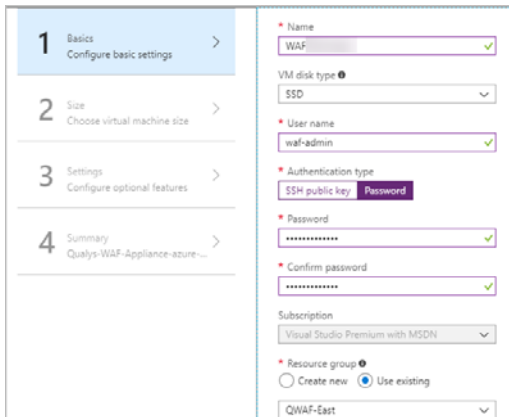
Don't see the WAF image?
Please contact your Technical
Account Manager or our
Support.

2) Create the WAF VM

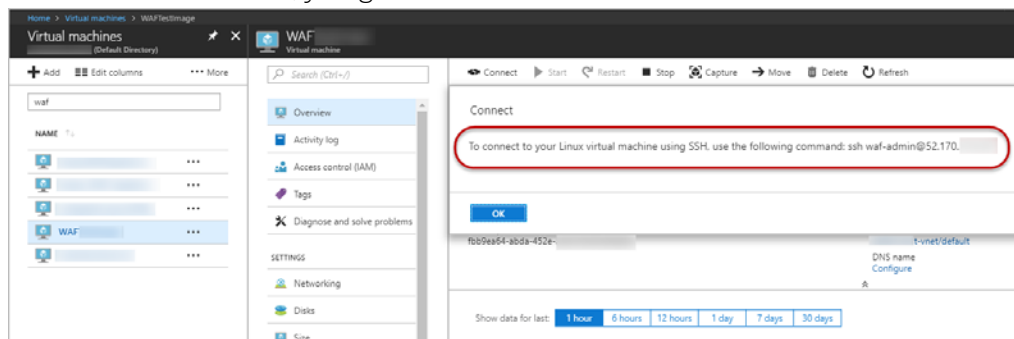
Click the WAF image, and then click Create VM.



Perform Steps 1 to 4 to provide the basic information, choose VM size, and configure network settings for the VM.



Once the VM is created, you get the ssh command to connect to the VM.



4) Register the appliance to Qualys Cloud Platform

Connect to the WAF VM and using the CLI enter your WAF registration code and other properties as appropriate. See [WAF registration parameters](#).

That's it! You've configured your WAF virtual appliance. Your WAF appliance will start making outbound connections to the Qualys Cloud Platform (HTTPS over TCP-443).

Google Cloud Configuration

Follow the steps below to deploy your WAF firewall on Google Cloud Platform (GCP).

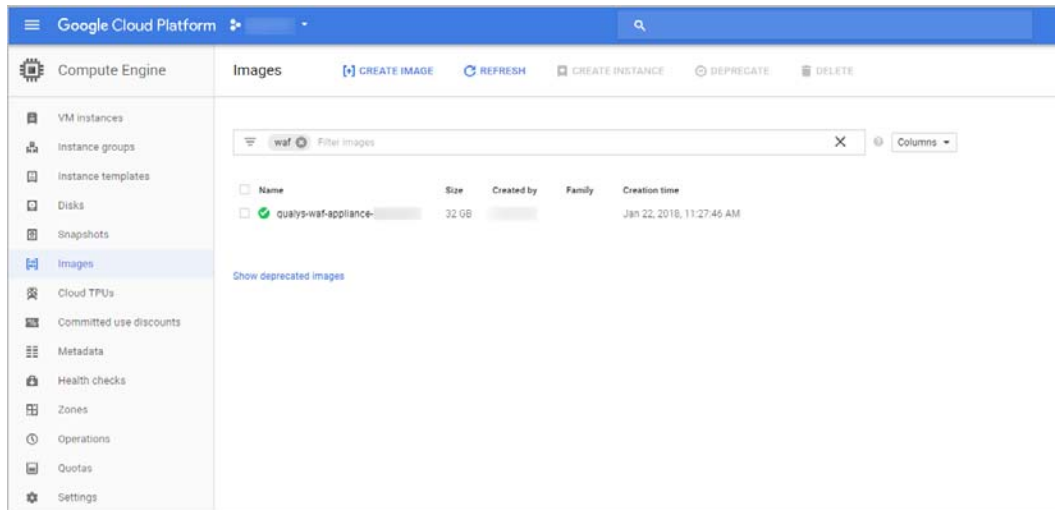
Once you complete these steps, we'll start monitoring your web application for security violations. Also your WAF appliance will start making outbound connections to the Qualys Cloud Platform for regular health checks - these confirm the appliance is properly configured and has the latest software.

Deploy WAF on Google Cloud Platform

1) Go to your GCP Dashboard and under Images find the Qualys WAF image.

Click Images and then search for the WAF image.

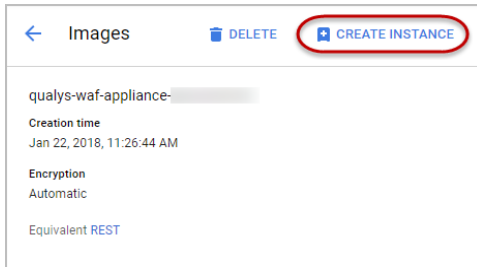
Tip Use the search box to find this quickly. Just enter “WAF” and click Enter.



Don't see the WAF image? Please contact your Technical Account Manager or our Support.

2) Create the WAF Instance

Click the WAF image, and then click CREATE INSTANCE.



Provide the basic information, choose Machine type, and configure access and network settings for the instance.

The screenshot shows the 'Create an instance' form. The form is titled 'Create an instance' with a back arrow. It contains several sections: 'Name' with a text input field containing 'instance-14'; 'Zone' with a dropdown menu set to 'us-central1-b'; 'Machine type' with a dropdown set to '1 vCPU' and '3.75 GB memory', with a 'Customize' link; 'Container' with a checkbox 'Deploy a container image to this VM instance' and a 'Learn more' link; 'Boot disk' with a 'New 32 GB standard persistent disk' and an 'Image' dropdown set to 'qualys-waf-appliance', with a 'Change' button; 'Identity and API access' with a 'Service account' dropdown set to 'Compute Engine default service account' and 'Access scopes' with radio buttons for 'Allow default access' (selected), 'Allow full access to all Cloud APIs', and 'Set access for each API'; and 'Firewall' with a note 'Add tags and firewall rules to allow specific network traffic from the Internet'. On the right side of the form, the estimated cost is shown as '\$25.55 per month estimated' and 'Effective hourly rate \$0.035 (730 hours per month)', with a 'Details' link.

3) Register the appliance to Qualys Cloud Platform

You can provide the WAF registration details while creating the instance or later once the instance is created.

To provide WAF registration details during instance creation, enter the variable and values in the form of key value pairs in the Metadata section.

Automation

Startup script (Optional)
You can choose to specify a startup script that will run when your instance boots up or restarts. Startup scripts can be used to install software and updates, and to ensure that services are running within the virtual machine. [Learn more](#)

Metadata (Optional)
You can set custom metadata for an instance or project outside of the server-defined metadata. This is useful for passing in arbitrary values to your project or instance that can be queried by your code on the instance. [Learn more](#)

Key	Value

[+ Add item](#)

Availability policy

Preemptibility
A preemptible VM costs much less, but lasts only 24 hours. It can be terminated sooner due to system demands. [Learn more](#)

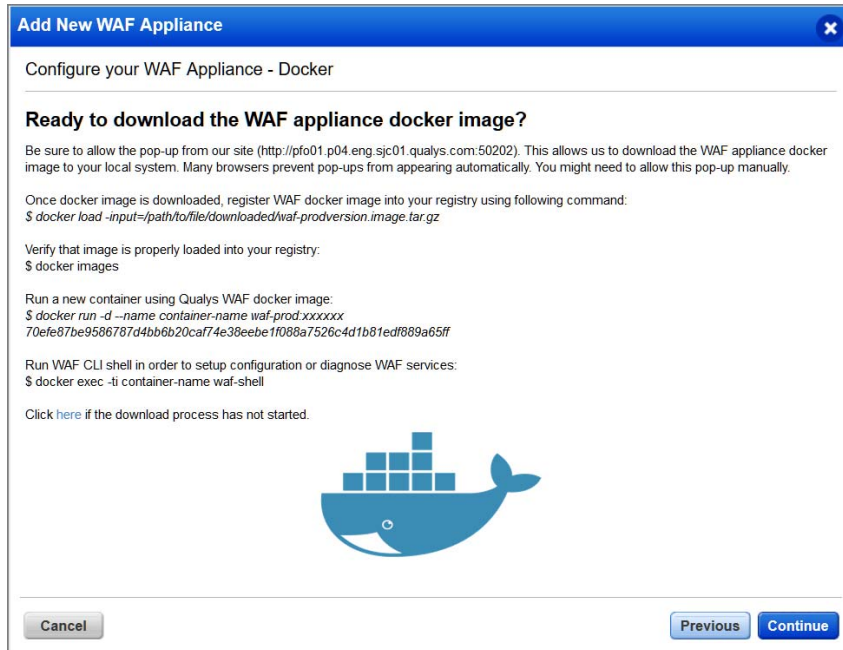
To register a WAF appliance once the instance is created, connect to the WAF instance and using the CLI enter your WAF registration code and other properties as appropriate. See [WAF registration parameters](#).

That's it! You've configured your WAF virtual appliance. Your WAF appliance will start making outbound connections to the Qualys Cloud Platform (HTTPS over TCP-443).

Docker Configuration

You can install the WAF appliance on a docker container.

Go to WAF Appliances > WAF Appliances, and click New WAF Appliance. Select an existing WAF cluster or create a new one. In the Add New WAF Appliance wizard, select Docker and click Continue to download the docker image file.



Refer to the onscreen instructions to create a container from the docker image. Click Continue to get the registration code of the cluster to register the WAF appliance to. See [CLI Reference](#) for information on registering the WAF appliance through CLI.

Ensure that the docker container has proper network connectivity for WAF appliance to communicate and register with the Qualys Cloud Platform (WAF_SERVICE_URL) in order to start sending WAF events.

CLI Reference

The command line interface is used to set up the WAF appliance. [Commands](#) and [Variables](#) are described below.

Commands

Command	Description
help	List all commands or give detailed help for a specific command. For more information about a command, type help followed by the command.
deregister	De-registers the sensor from its cluster and shutdown.
diag [details]	Simple diagnostic tool (nslookup, perfstat, fetchurl, ssl). Example to forge a specific servername value (SNI): <code>diag ssl www.domain.com:443 "foo.domain.com"</code> Example to forge a specific host header value: <code>diag fetchurl https://servername.domain.com "Host: foo.domain.com"</code>
exit	Exit the CLI. The user will be prompted if there are unsaved changes.
ifconfig	Show the current interface configuration.
network	Configure the network interface, i.e. add, change, delete network route, and set nameservers to be used.
passwd	Change the password for user waf-user.
reboot	Reboot the WAF cluster.
routes	Show network routing.
save	Save the current configuration.
set variable ={value}	Set a key value for configuration.
setup	Helps you set up properties by prompting for registration code, WAF service URL, proxy URL and SSL passphrase.
show [details]	Show the current saved and unsaved settings. Show details will include settings from the virtualization platform.
shutdown	Shutdown the WAF sensor.
ssh	Configure the public ssh keys, i.e. add, delete, list.
status	Display the registration status of the WAF cluster.
sysinfo	Display system information.
viewlog [n]	View the last N lines of the WAF cluster log.
waf	Manage the WAF process, i.e. start, stop, restart, reconfigure, get status.

Command	Description
unset variable	Clear the value for a variable.
ca	Add, Delete or List CA certificates.
core [status enable disable]	Enable or disable generating the core dump file upon crash. By default core is enabled.

Variables

Variable	Description
waf_service_url	(Required) The URL of the Qualys Cloud Platform hosting your Qualys account. Supported platform URLs are: US Platform 1 https://rns.qualys.com US Platform 2 https://rns.qg2.apps.qualys.com US Platform 3 https://rns.qg3.apps.qualys.com EU Platform 1 https://rns.qualys.eu EU Platform 2 https://rns.qg2.apps.qualys.eu India Platform 1 https://rns.qg1.apps.qualys.in
registration_code	(Required) Enter the WAF registration code in this format: registration_code=your_code. You can find this code by going to the WAF clusters list (WAF Appliances > WAF Clusters).
proxy_url	(Required if a proxy is required for the WAF cluster to access the Qualys Cloud Platform) If the WAF needs to connect to the Qualys Cloud Platform through an HTTP proxy, please input the URL of the proxy. Enter the proxy URL in this format: proxy_url=proxy_url
waf_ssl_passphrase	(Required if the appliance protects a site communicating over SSL) If your web application's primary or secondary base URL uses the HTTPS protocol, the Qualys Cloud Platform portal protects the private key by encrypting it with a 64 byte dedicated passphrase. This way, it's not accessible in clear on the Qualys Platform. This waf_ssl_passphrase needs to be set on the appliance, for decrypting the key. Enter the passphrase in this format: waf_ssl_passphrase=passphrase
sem_syslog_addr	The Security Event Manager to send transaction logs via syslog to. The syslog messages will be formatted as described in RFC5424. Syntax: PROTOCOL:HOSTNAME:PORT where PROTOCOL is "tcp" or "udp", and PORT is standard syslog port 514 by default Example: TCP:sysloghost.example.com:514

Contact Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access online support information at www.qualys.com/support/.