# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Why Use a Web Application Firewall</td>
<td>4</td>
</tr>
<tr>
<td>The Qualys Advantage</td>
<td>5</td>
</tr>
<tr>
<td><strong>Get Started</strong></td>
<td>6</td>
</tr>
<tr>
<td>Create WAF Cluster</td>
<td>7</td>
</tr>
<tr>
<td>Explore Security Policies</td>
<td>9</td>
</tr>
<tr>
<td>Create application profiles</td>
<td>10</td>
</tr>
<tr>
<td>Web Server Pool Profile</td>
<td>10</td>
</tr>
<tr>
<td>Healthcheck Profile</td>
<td>11</td>
</tr>
<tr>
<td>SSL Certificate Profile</td>
<td>12</td>
</tr>
<tr>
<td>Custom Response Pages</td>
<td>13</td>
</tr>
<tr>
<td>HTTP Profile</td>
<td>14</td>
</tr>
<tr>
<td>Define Your Web Application</td>
<td>15</td>
</tr>
<tr>
<td>Configure WAF Appliance</td>
<td>18</td>
</tr>
<tr>
<td>Configure Your Web Environment</td>
<td>20</td>
</tr>
<tr>
<td>We’re Now Monitoring Your Web Application!</td>
<td>21</td>
</tr>
<tr>
<td>Add Exceptions</td>
<td>22</td>
</tr>
<tr>
<td>Add Virtual Patches</td>
<td>22</td>
</tr>
<tr>
<td>Add Custom Rules</td>
<td>23</td>
</tr>
<tr>
<td>Upgrading WAF Cluster - Scanner Appliances</td>
<td>26</td>
</tr>
<tr>
<td>VMware and Hyper-V Configuration</td>
<td>27</td>
</tr>
<tr>
<td>Import and Register your WAF Appliance</td>
<td>27</td>
</tr>
<tr>
<td>Set Up the Appliance using the CLI</td>
<td>29</td>
</tr>
<tr>
<td>Reboot may be required</td>
<td>30</td>
</tr>
<tr>
<td>Verify Registration</td>
<td>30</td>
</tr>
<tr>
<td>Amazon EC2 Configuration</td>
<td>31</td>
</tr>
<tr>
<td>Launch New EC2 Instance</td>
<td>31</td>
</tr>
<tr>
<td>Add Your WAF AMI to the Load Balancer</td>
<td>34</td>
</tr>
<tr>
<td>CLI Reference</td>
<td>36</td>
</tr>
<tr>
<td>Commands</td>
<td>36</td>
</tr>
<tr>
<td>Variables</td>
<td>38</td>
</tr>
<tr>
<td>Contact Support</td>
<td>39</td>
</tr>
</tbody>
</table>
Why Use a Web Application Firewall

HTTP(S) is the foundation of data communication for the World Wide Web, and functions as a request-response protocol for communications. Mobile apps, cloud computing, API communications, Intranet applications and webmail are common tools we use every day. These applications are all communicating over HTTP(S).

Qualys provides applications that allow you to scan and identify vulnerabilities - Qualys Vulnerability Management (VM) and Qualys Web Application Scanning (WAS).

Experience shows that patching web site source code can take longer than expected, depending on the affected component, development resources, and how agile the company is in applying and validating software updates.

That’s where Qualys Web Application Firewall (WAF) comes in. This is an immediate remediation tool that is able to protect your web applications against attacks and gives your development team time to fix important security issues.

Using WAF users can deploy multiple firewall instances for their web applications. Each firewall consists of a virtual appliance that is configured to reverse proxy your HTTP(S) traffic. This appliance will be located in your virtualization platform (Amazon EC2, VMware or Hyper-V) and will be instantiated from a Qualys machine image. We’ll walk you thru the steps in this user guide.
The Qualys Advantage

Qualys offers a powerful, next generation web application firewall that uses an always up to date security ruleset to secure your web applications. This modern firewall uses a cloud-based approach and provides a classic mode of operation and deployment.

All security events are routed through the Qualys Cloud Platform. They are continuously monitored and analyzed by our security researchers in order to compute the best ruleset for blocking the latest attacks and zero-day vulnerabilities. Qualys WAF users set up security policies for their web applications based on rules to filter, monitor, block and report on events.

Qualys WAF makes it easy to understand the security of all your web applications at once. A concise visual dashboard summarizes the various events that have occurred, when they took place and where they came from. Easily get interactive insights into potential threats and find detailed information on each potential threat and how to address it.
Get Started

Start protecting your web applications and blocking attacks now! We’ll help you do this quickly.

Log in to your Qualys account and choose WAF

You’ll see our Quick Start Guide the first time you log in - just follow the steps to get started. You’ll find tutorials and links to other helpful information.

Tip: Get back to the Quick Start Guide anytime - it’s on the user name menu.
Create WAF Cluster

A WAF cluster is the pivot between the web application and the appliance it is being proxied through. It is a group of one or more WAF appliances (or proxy-set). A WAF Cluster can contain several appliances, but each will act as standalone, while processing the traffic exactly the same way across all the appliances that are registered with the named Cluster. A Web Application can be proxied over several clusters.

It’s easy to create a WAF Cluster. Go to WAF Appliances > WAF Clusters and click the New WAF Cluster button.

Enter an arbitrary name. To help with cluster management you can add description and assign tags.
For error responses you can choose to show the default WAF error page, or define a custom response or a redirection code (301 or 302) along with a location. Selecting Block will display the default WAF error page.

Whenever a request is addressed to a nonexistent FQDN, you can choose to display the default WAF error page, a custom response page or you can redirect the request towards a specified location. This happens if a malicious user forges a request with a false host header or the host requested is missing in the alias configured for your website.

Once created you’ll see your new WAF cluster in the list. The status ○ means the cluster does not have any WAF appliances assigned to it yet (we’ll do this soon).

Notice the Registration Code. You’ll use this to register your WAF cluster when you configure a WAF appliance.
Explore Security Policies

The security policy you assign to your web application determines the WAF inspection criteria and sensitivity level - this impacts what violation we’ll report for your web application and whether or not we’ll flag the traffic as malicious.

**Good to know**

Only one security policy can be assigned to each web application.

Choose from out-of-the-box policy templates provided by Qualys with this release - Drupal, Joomla, Wordpress, and OWA. Built-in Templates and System Policies are not modifiable.

Or start with a blank policy and customize the policy settings. You can create multiple policies and assign them to your various web applications (one to each web app).

Go to Security > Policies and click the New Policy button.

Our wizard will help you with the settings.

**Application Security** - Configure a sensitivity rating (20 to 80) for the various detection categories. This impacts what inspection will be performed by filtering potentially noisy events.

**Policy Controls** - Set threat level thresholds (1 to 100) for logging and blocking. This impacts what events we will log and block.
Create application profiles

Qualys WAF now allows you to create reusable profiles for settings which can be commonly used by multiple web applications. Reusable profiles can be created for Web server pools, healthcheck parameters, SSL certificates, and HTTP protocol filters.

Good to know

For each web application in your account you’ll assign 1 profile of each type, i.e. Web server pool, healthcheck, SSL certificate, and HTTP protocol filters.

Web Server Pool Profile

Don’t have a dedicated load balancer? No worries, with newly introduced web server pools, Qualys WAF can now load balance traffic between multiple origin servers. You can choose one web server pool per web application.

Go to Web Applications > Web Servers and click the New Web Servers button.

Add one or more servers in the pool, having common port and protocol. You can use weights for WAF to distribute the request load to various servers in the Web Server Pool. Simply add the weight (number) beside the server address. You can add weights to your existing pool as well. Default is 1. Maximum allowed value is 256.

Consider a pool consisting of four origin servers with the weights 1, 2, 3 and 3. The total weights assigned to all servers is 9. WAF distributes 1/9th of total load to server 1, then 2/9th of total load to server 2, and so on.

Then choose the load balancing method to determine which server receives the connection.
Healthcheck Profile
Create healthcheck profiles to monitor application’s availability against your web servers. You’ll choose one healthcheck profile per Web Application. It will be executed against all the web servers listed in the server pool, according to a user-defined frequency. If one backend web server fails the healthcheck after X attempts, it will be considered down and no request will be steered to it until the service is back. Meanwhile, the firewall will keep probing the backend.
Consequently, if all backend web servers fail the healthcheck, they will all be considered as down by the firewall, thus leading to application unavailability – meaning the WAF will stop forwarding the traffic on server-side. Instead, it will respond to the client with a user-defined HTTP response code. This “failure response code” is set within the Web Application itself, in the Application tab.

Go to Web Applications > Healthchecks and click the New Healthcheck button.

While creating a healthcheck profile, specify the preferred HTTP method to query the application, the URL path to be checked, and the response code returned for success. You can also specify the “up” and “down” intervals and occurrences to fix the frequency of the probes, along with the amount of successes or failures before changing backend web server’s status. Based on the healthcheck result, the server status is set to active or inactive.

The WAF appliances tab displays the healthcheck status for all servers covered by an appliance. This server healthcheck information is grouped by each web application that the appliance monitors.
SSL Certificate Profile

Declare SSL materials used by your web applications on client-side.

Go to Web Applications > SSL Certificates and click the New SSL Profile button.

Provide a PKCS12 file, or simply copy-paste the contents of the certificate, private key, and passphrase directly into the UI.

The private key will be encrypted with the newly generated WAF SSL Passphrase. Copy-paste the 64 byte passphrase to your appliance “waf_ssl_passphrase” environment variable. See CLI Reference for details.
Custom Response Pages
Display a custom page instead of the default WAF error page, if your security policy blocks a particular section or a page on your website or if a request cannot be routed to your origin server.

Go to Web Applications > Custom Response Pages and click the New Custom Response Page button.

In the Configuration panel’s Response Page Body, paste your response in HTML format.

This custom response can now be reused for multiple web applications and appliance clusters. Simply select your custom response page in the web application wizard, and the WAF cluster wizard.
HTTP Profile
Set up an HTTP profile to filter protocol oriented attributes (methods, content-type, declarative security, and information leakage attributes). You can choose one HTTP profile per web application.

Go to Security > HTTP Profiles and click the New HTTP Profile button.

HTTP Protocol - Configure HTTP protocol analysis for the policy.

Information Leakage - Choose options for server cloaking, sensitive header suppression, error messages and sensitive file requests.

Declarative Security - Configure responses to cookies, content-type sniffing and browser cross-site scripting.
Define Your Web Application

Tell us about the web application you want to monitor.

Go to Web Applications and click the New Web Application button.

Choose Blank and we’ll help you build the web asset from scratch.

Tip Is the web asset already in your subscription? Use Existing Asset to save time! (You’ll just enter WAF settings)
1) **Asset Details** Give your web asset a name, tell us the primary URL, add custom attributes if any, and assign tags (optional)

![Image of Asset Details](image1)

**Tip** Turn on help tips (in the title bar) and we’ll show you useful tips as you hover over the various settings.

2) **Application** Set secondary URLs, and then select the reusable profiles created for Web Server pool and SSL Certificate. You can create new profiles directly from this wizard.

![Image of Application](image2)

**Tip** Optionally select a Healthcheck profile and set the failure response code.

3) **Security** Select an action, and then select or create security policy and HTTP profiles. Selecting Block with Custom Response allows you to display a custom message to the user if your security policy blocks a particular section or a page on your web site. Select a custom response page that you have created.
Then add one or more custom rules to allow or block access to certain web application resources.

4) **WAF clusters** Select a cluster to deploy your web app in. A cluster contains one or more appliances (reverse-proxies).

It’s possible for multiple WAF clusters to monitor the same web application.

Once your web application is created it shows up on the UI under the Web Applications tab. To view information about various web application statuses and their meanings, click Help > Online Help and then on the Start monitoring your web applications page, click **Tell me about status**.
Configure WAF Appliance

You’ll add a WAF virtual appliance and configure it for your WAF cluster within your environment - Amazon EC2, VMware or Microsoft Hyper-V.

Good to know

A WAF cluster can be assigned as many WAF appliances as your subscription allows guaranteeing high availability and/or fault tolerance in your firewalling operations.

Tell me the steps

1) Add a new WAF Appliance for your WAF cluster. Just go to WAF Appliances > WAF Appliances, click New WAF Appliance, and we’ll walk you through the steps.

2) Configure the WAF appliance for your environment. See our step by step instructions:

Amazon EC2 Configuration

VMware and Hyper-V Configuration

Once your appliance is registered it shows up on the UI under the WAF Appliances tab. To view information about various appliance statuses and their meanings, click Help > Online Help and then on the Configure WAF appliances page, click Tell me about appliance status.

Firewall rules / EC2 security groups

- Allow HTTP(S) traffic (TCP-80,443; or any other) to the WAF appliance from Internet.
- Allow SSH (TCP-22) to the WAF appliance from a trusted management network only.
- Allow minimum access to the origin web server(s): only the WAF appliance ip address should be granted access to web servers’ production [ip:port]. Any direct access should be strictly limited to the administration network only.

Load balancer considerations

- Load balancers should be configured to hand off to WAF cluster nodes so we can appropriately configure redundancy within the infrastructure.
- The WAF appliance functions as a reverse proxy. It is important that any DNS configurations, firewall NAT or load balancer configurations are set to forward traffic towards the WAF appliance. It will then inspect incoming request, and based on your configuration, hand it off to the appropriate origin server.
Upgrading WAF appliances

We regularly release scanner appliance software to bring you our latest features and improvements. When software updates are available use the cluster Upgrade option to upgrade all Scanner Appliances registered to that cluster. See Upgrading WAF Cluster - Scanner Appliances.
Configure Your Web Environment

Be sure to get traffic to your WAF appliance - configure load balancers and/or DNS as needed to direct traffic to your WAF cluster for inspection.

We recommend you check to be sure your WAF cluster has an active status. Go to WAF Appliances > WAF Clusters.

- Status ○ means the cluster does not have any WAF appliances assigned to it.
- Status ☑ means the cluster has appliances registered, none are inactive, and the cluster protects at least one site.

Sample WAF Clusters list
We’re Now Monitoring Your Web Application!

Check out the security events (violations) we’ve found on your web application. To discover more about an event, hover over it and choose View Event Details from the menu.

You can view detailed information about each potential threat. Review the event details and take actions from the menu, i.e. mark the event as Flagged, False Positive, or Not Applicable. Tip - Clicking on a QID will take you to Qualys comprehensive KnowledgeBase which provides additional information about each threat and how to address it.
Add Exceptions

Use Exceptions when you identify a false-positive or false-negative event. A false-positive is a legitimate request that has been unexpectedly blocked. A false-negative is a non-legitimate request that has been authorized while it shouldn’t have.

With Qualys WAF you can flag an event as a false-positive. To do that, go to Events > Event List, select an event, click on the arrow and select “Mark as False positive”. Bear in mind this is a simple marker, it does not impact traffic processing behavior.

To create an exception, select an event, click on the arrow and select “Create exception”.

Add Virtual Patches

Use Virtual Patches upon vulnerability detection by the Web Application Scanning module. To do that, select the WAS module, go to Web Applications > Detections, click on the arrow and select “Install Patch”.
Add Custom Rules

Use Custom Rules to define static traffic workflow. Rules allow you to fully control HTTP transactions in order to adapt the security policy in effect for enterprise constraints. Custom rules replace previous Access Rules and Control Rules.

Go to Security > Rules and click the New Custom Rule button.

We have provided various keys to form conditions for a rule.

Want to see all the available keys? Simply place the cursor in the When field, and press the down arrow key on your keyboard to get a list of all available keys. Syntax help is available for every key.

How do I get started? Press the Down arrow to see the available keys.
How do I add a condition?

- Select a key like client.ip.address.
- Then select an operator.

- Enter a value for your condition in double quotes. In this case we've entered an IP address.

- Press Enter to add your condition. It will look like this.

- Click the Add button to add another condition to your rule.
- Complete the steps to add conditions as needed.
We’ve added 3 conditions for our rule.

Here’s the conditions:

\[
\begin{align*}
\text{client.ip.address} & \text{ EQUAL } "172.26.10.123" \\
\text{client.tcp.port} & \text{ EQUAL } "45678" \\
\text{transaction.day} & \text{ EQUAL } "Sunday"
\end{align*}
\]

How does this rule work? The rule gets executed only when all conditions are met. Otherwise, the rule gets ignored.

In the actions panel of the wizard, you tell us what action to take when events match the conditions in the rule.

Once created, assign one or more rules to your web application from within the web application wizard. Rules are executed in the order defined in web application settings.

**Good to know**

Rules are parsed from top to bottom, in the order defined in web application settings. Custom rules support regular expressions with PCRE. Character escaping is possible with the backslash (\).
Upgrading WAF Cluster - Scanner Appliances

Our service regularly releases scanner appliance software to bring you our latest features and improvements. When software updates are available use the cluster Upgrade option to upgrade all Scanner Appliances registered to that cluster.

The WAF Scanner Appliances by Version graph tells you whether there's software updates available for your Scanner Appliances. You will see the number of appliances running the latest or outdated versions.

To upgrade a WAF cluster, go to WAF Appliances > WAF cluster, and then click Upgrade in the Quick Actions menu of the cluster that you want to upgrade.

You get a confirmation message displaying the number of appliances registered to the cluster. Click Confirm to upgrade.

To verify successful upgrade, check the WAF Scanner Appliances by Version graph. The number of appliances you have upgraded should get added to the number of Appliances with latest version or higher.
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.


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.

```bash
$ 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`. More properties may be required depending on your networking environment. See CLI Reference for details.

```bash
$ 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.
```

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.
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
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 using the variables below.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAF_SERVICE_URL</td>
<td>(Required) The URL of the Qualys Cloud Platform hosting your Qualys account. Supported platform URLs are:</td>
</tr>
<tr>
<td></td>
<td>US Platform 1  <a href="https://rns.qualys.com">https://rns.qualys.com</a></td>
</tr>
<tr>
<td></td>
<td>US Platform 2  <a href="https://rns.qg2.apps.qualys.com">https://rns.qg2.apps.qualys.com</a></td>
</tr>
<tr>
<td></td>
<td>EU Platform 1  <a href="https://rns.qualys.eu">https://rns.qualys.eu</a></td>
</tr>
<tr>
<td></td>
<td>EU Platform 2  <a href="https://rns.qg2.apps.qualys.eu">https://rns.qg2.apps.qualys.eu</a></td>
</tr>
<tr>
<td></td>
<td>India Platform 1 <a href="https://rns.qg1.apps.qualys.in">https://rns.qg1.apps.qualys.in</a></td>
</tr>
<tr>
<td>REGISTRATION_CODE</td>
<td>(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 &gt; WAF Clusters).</td>
</tr>
<tr>
<td>PROXY_URL</td>
<td>(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</td>
</tr>
<tr>
<td>WAF_SSL_PASSPHRASE</td>
<td>(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</td>
</tr>
</tbody>
</table>

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](#)

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.

### Listener Configuration:

<table>
<thead>
<tr>
<th>Load Balancer Protocol</th>
<th>Load Balancer Port</th>
<th>Instance Protocol</th>
<th>Instance Port</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>80</td>
<td>HTTP</td>
<td>80</td>
<td>Remove</td>
</tr>
</tbody>
</table>

![Create a New Load Balancer](#)

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](#)
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.

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.

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).
# CLI Reference

The command line interface is used to set up the WAF appliance. Commands and Variables are described below.

## Commands

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>waf_service_url</td>
<td>(Required) The URL of the Qualys Cloud Platform hosting your Qualys account. Supported platform URLs are:</td>
</tr>
<tr>
<td></td>
<td>US Platform 1         <a href="https://rns.qualys.com">https://rns.qualys.com</a></td>
</tr>
<tr>
<td></td>
<td>US Platform 2         <a href="https://rns.qg2.apps.qualys.com">https://rns.qg2.apps.qualys.com</a></td>
</tr>
<tr>
<td></td>
<td>EU Platform 1         <a href="https://rns.qualys.eu">https://rns.qualys.eu</a></td>
</tr>
<tr>
<td></td>
<td>EU Platform 2         <a href="https://rns.qg2.apps.qualys.eu">https://rns.qg2.apps.qualys.eu</a></td>
</tr>
<tr>
<td></td>
<td>India Platform 1     <a href="https://rns.qg1.apps.qualys.in">https://rns.qg1.apps.qualys.in</a></td>
</tr>
<tr>
<td>registration_code</td>
<td>(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 &gt; WAF Clusters).</td>
</tr>
<tr>
<td>proxy_url</td>
<td>(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</td>
</tr>
<tr>
<td>waf_ssl_passphrase</td>
<td>(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</td>
</tr>
<tr>
<td>sem_syslog_addr</td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>Example: TCP:sysloghost.example.com:514</td>
</tr>
</tbody>
</table>
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/.