IMPERVA®

SecureSphere

WAF on AWS Deployment Kit

Instructions

May 2016

Copyright Notice

Imperva Inc.

3400 Bridge Parkway, Suite 200

Redwood Shores, CA 94065

United States

Tel: +1 (650) 345-9000
Fax: +1 (650) 345-9004

- **Website**: http://www.imperva.com
- **General Information**: info@imperva.com
- **Sales**: sales@imperva.com
- **Professional Services**: consulting@imperva.com
- **Technical Support**: support@imperva.com

Imperva-SecureSphere-v11.5-WAF-on-Amazon-AWS-Deployment-Kit-Instructions-v1.0

End User License and Services Agreement

To view the End User License and Service Agreement for this product, please visit
http://www.imperva.com/Other/LicenseAgreement

AWS Deployment Kit Supported Platforms

The AWS Deployment Kit is supported with the following 'SecureSphere on AWS' platforms:

- **SecureSphere Versions**: v11.5
- **License Models**: Both BYOL and On-Demand
- **Products**: WAF

Using the SecureSphere AWS Deployment Kit

The AWS Deployment Kit is a special CloudFormation template file that enables the user to create a working AWS environment, complete with availability zone redundancy, scalable Gateways, a working accessible Management Server, NAT instances, Load balancers etc., in about 90 minutes.

The Deployment Kit can be used to set up a real, production deployment, or it can be used by customers who need more information on what a deployment should look like by creating a working reference deployment, to which they can then refer in order to troubleshoot their own SecureSphere AWS deployment.

The Deployment Kit sets up the following components:

- **VPC**: a virtual private cloud network
- **2 NAT instances**: required in order to allow access to Amazon API commands for the creation of the Management Server and the Gateway, as well as provide access to the Management Server UI
- **2 management subnets**: used to access the Management server, one for each availability zone;
- **2 data subnets**: used by the Gateway instances, one for each availability zone
- **2 public subnets**: used by the NAT instances, one for each availability zone
- **Management Server stack**: an AWS stack that creates our Management Server
- **Gateway stack**: an AWS stack that creates a scaling group of Gateways on 2 availability zones
- **ELB**: a load balancer that directs HTTP traffic to the Gateways
- **Routing tables**: for each subnet mentioned above, a routing table is needed to allow access to other subnets
- **Security groups**: facilitate and block traffic from specific ports and subnets.

Note that the Deployment Kit creates a fixed setup with the following characteristics:

- It sets up NAT instances rather than an HTTP Proxy
- It creates two Gateways in two availability zones
- It sets up a Management Server with no MX-HA
- It creates a single VPC and multiple subnets, and does not use existing VPCs or subnets
- It protects servers exposed to the internet and not a web server inside the VPC. You can easily update the deployment to support internal servers by VPC peering or using a VPN to the new VPC.

Deploying SecureSphere WAF with the AWS Deployment Kit

Deploying SecureSphere WAF with the AWS deployment kit is designed to be seamless and fast, but it creates a very specific setup of SecureSphere.

Before you begin this procedure, obtain a license from Imperva. For more information, see Licensing SecureSphere.

To deploy SecureSphere WAF with the AWS deployment kit:

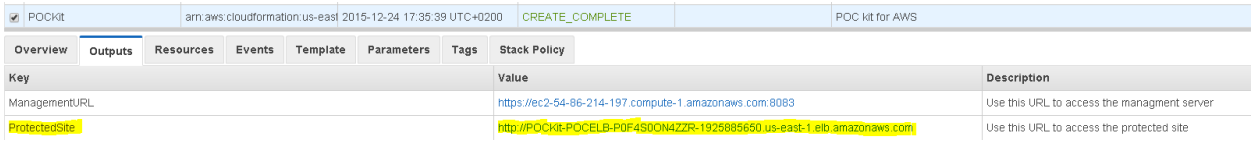
1. In your browser, navigate to your Amazon Web Services page, and log in using your AWS account information.
2. Under **Deployment and Management**, click **CloudFormation**. The **CloudFormation** page appears.
3. Click **Create Stack**. The **Select Template** page appears.
4. Under **Template**, select **Upload a template to Amazon S3** and click **Browse**. The **File Upload** dialog box appears.
5. Navigate to the AWS development kit json file (SecureSphere-POC-Kit-<SecureSphere-Version>.json) on your computer, then click **Open**. The dialog box closes.
6. In the **Select Template** page, click **Next**.
7. Enter a **Stack Name** for your stack.
8. Under **Parameters**, enter values in accordance with the table below. Click **Next**. The **Options** page appears.
9. Optional - Under **Tags**, for **Key** enter `Name`, and for **Value** enter the name you gave the stack.
10. Click **Next**. The Review page appears, summarizing the values for the parameters of your new stack.
11. Review these values to ensure they are correct.
12. Check the box **I acknowledge that this template might cause AWS CloudFormation to create IAM resources**. Click **Create**. The **CloudFormation** page appears, showing the progress of the creation of your new stack.

    The development kit first creates the Management Server stack, and then the Gateway stack. The process takes about 90 minutes.

Name	Description
KeyPairName	The AWS Key pair for connecting to the NAT instances and SecureSphere servers.
LicenseURL	The URL for the license file.
MXPassword	The password used to log in as an **admin** user to the Management Server UI.
ProtectedSite	The address of a site that the user would like SecureSphere to protect.

Confirming that the SecureSphere WAF Site is Running

When the AWS development kit set-up process is complete, you can confirm that the site is running by selecting the **Output** tab.



- **ManagementURL**: The link to the Management Server UI, that enables you to manage your SecureSphere system.
- **ProtectedSite**: The link to the protected site.

Notes:

- The AWS development kit creates a forwarding rule in the NAT instance to allow external access to the Management Server port. For production environments, remove this and ensure that the Management Server is accessible by internal connections (e.g. jump server) only.
- The NAT instance's DNS name may change after reboot. This new DNS name will not appear in the value of the **ManagementURL**. You can find the new name in the EC2 console.

Moving to Production

If you want to make your deployment kit setup into a production setup, you should consider carrying out the following tasks:

- **Remove external access to the Management Server**: The AWS development kit creates a forwarding rule in the NAT instance to allow external access to the Management Server port. For production environments, remove this and ensure that the Management Server is accessible by internal connections (e.g. jump server) only.
- **Protect internal servers**: You need to configure your web application servers so that they receive traffic via the WAF only. The WAF should then be connected to the web servers' VPC. this can be achieved by VPC peering. For more information, see VPC Peering.
- **Move to protection**: For more information, see Configuring Operation Mode.
- **Configure XFF**: For more information, see XFF.