Check Point CloudGuard Auto Scaling on the AWS Cloud

Quick Start Reference Deployment

September 2019

Check Point Software Technologies
AWS Quick Start Reference Team

Contents

This Quick Start deployment guide was created by Check Point Software Technologies in collaboration with Amazon Web Services (AWS).

Quick Starts are automated reference deployments that use AWS CloudFormation templates to deploy key technologies on AWS, following AWS best practices.

Overview

This Quick Start reference deployment guide provides step-by-step instructions for deploying a web service secured by an Auto Scaling group of Check Point CloudGuard Security Gateways on the AWS Cloud.

AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. For example, a web application might be served by multiple web servers that are deployed across multiple Availability Zones.

This Quick Start is for users who want to publish an automatically scaled and dynamically secured web service on AWS, defining content-level access policy, monitoring incoming requests to the service, applying intrusion prevention system (IPS) protections for web servers, enforcing geo-based policy, preventing malicious bots activity, and more.

The Quick Start deploys an Auto Scaling group of Check Point CloudGuard Security Gateways in front of a workload of web servers, because a security solution should be as scalable as the setup it is protecting. Additionally, you can select to deploy either an external Application Load Balancer that operates at the application layer, or a Network Load Balancer that operates at the transport layer, to route traffic from the internet to the Security Gateways.

To manage the CloudGuard Security Gateways, you can choose to deploy a preconfigured Check Point CloudGuard Security Management Server, use an existing Security Management Server, or deploy one later.

If you choose to deploy your workload of web servers, this Quick Start will also deploy an internal Application Load Balancer, to route traffic from the Security Gateways to your

workload. Otherwise, you can use existing internal load balancers, or deploy those later, by tagging them in the AWS Management Console.

> **Note** This Quick Start uses externally hosted CloudFormation templates that deploy additional resources. The templates are provided and maintained by Check Point.

Check Point CloudGuard for AWS

Check Point CloudGuard for AWS extends comprehensive threat prevention security to the AWS Cloud. It protects assets in the cloud from attacks while enabling secure connectivity.

CloudGuard lets you enforce consistent security policies across your entire organization by protecting data between the corporate network and your virtual private cloud (VPC). CloudGuard can also inspect data entering and leaving the private subnet in the VPC to prevent attacks and to mitigate data loss or leakage.

Check Point CloudGuard for AWS meets an organization's cloud security needs with flexible and manageable security options, including Firewall, Intrusion Prevention System (IPS), Application Control, Antivirus, Anti-Bot, URL filtering, Identity Awareness, advanced Threat Prevention, and Threat Extraction Software for known threats and zero-day attacks. CloudGuard protects services in the public cloud from the most sophisticated threats and from unauthorized access while preventing application layer denial-of-service attacks.

Costs and Licenses

You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using the Quick Start.

The AWS CloudFormation template for this Quick Start includes configuration parameters that you can customize. Some of these settings, such as instance type, will affect the cost of deployment. For cost estimates, see the pricing pages for each AWS service you will be using. Prices are subject to change.

The Check Point CloudGuard Security Gateways, which are launched by the Auto Scaling group deployed in this Quick Start, and the optional Check Point CloudGuard Security Management Server, require a license.

Because this Quick Start uses Amazon Machine Images (AMIs) from AWS Marketplace, you must subscribe to Check Point CloudGuard in AWS Marketplace before you launch the

Quick Start. There are two licensing options: Pay As You Go (PAYG) and Bring Your Own License (BYOL). See step 2 in the deployment section for details and links.

To purchase BYOL licenses, contact Check Point Sales. If you already have a BYOL license and you'd like to use it for this deployment, visit the Licensing section of Check Point's *CloudGuard Auto Scaling in AWS* documentation.

Architecture

Deploying this Quick Start for a new virtual private cloud (VPC) builds the following Check Point CloudGuard Auto Scaling environment in the AWS Cloud.

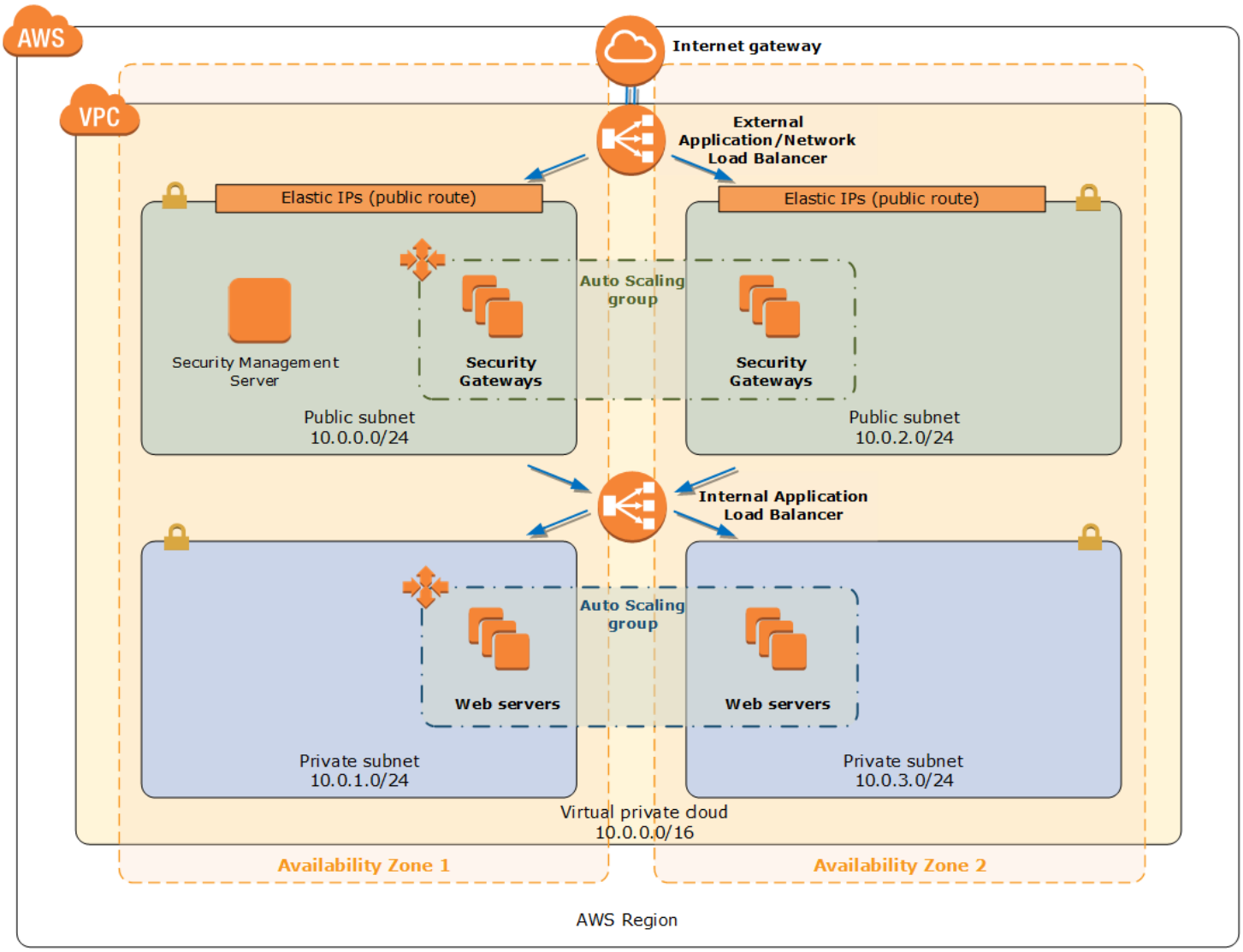


Figure 1: Quick Start architecture for Check Point CloudGuard Auto Scaling on the AWS Cloud

The Quick Start sets up the following:

- A highly available architecture that spans at least two Availability Zones.*
- A VPC configured with public and private subnets according to AWS best practices, to provide you with your own virtual network on AWS.*
- An internet gateway to allow access to the internet. This gateway is used by the CloudGuard Security Gateways to send and receive traffic.*
- In the public subnets, CloudGuard Security Gateways in an Auto Scaling group.
- Either an external Application Load Balancer that operates at the application layer or a Network Load Balancer that operates at the transport level, to route traffic from the internet to the CloudGuard Security Gateways.
- In a public subnet, an optional, preconfigured CloudGuard Security Management Server, to manage the Security Gateways.
- In the private subnets, an optional Auto Scaling group of web servers.
- If you choose to deploy your workload of web servers, an internal Application Load Balancer, to route traffic from the Security Gateways to your workload.

* The template that deploys the Quick Start into an existing VPC skips the tasks marked by asterisks and prompts you for your existing VPC configuration.

Prerequisites

Specialized Knowledge

Before you deploy this Quick Start, we recommend that you become familiar with the following AWS services. (If you are new to AWS, see Getting Started with AWS.)

- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic Block Store (Amazon EBS)
- Amazon Simple Notification Service (SNS)
- Amazon VPC
- AWS CloudFormation
- AWS Auto Scaling
- AWS Identity and Access Management (IAM)
- Elastic Load Balancing

Deployment Options

This Quick Start provides two deployment options:

- **Deploy Check Point CloudGuard Auto Scaling into a new VPC** (end-to-end deployment). This option builds a new AWS environment consisting of the VPC, subnets, security groups, load balancers, and other infrastructure components, and then deploys the Auto Scaling group of Check Point CloudGuard Security Gateways into this new VPC.
- **Deploy Check Point CloudGuard Auto Scaling into an existing VPC**. This option deploys an Auto Scaling group of Check Point CloudGuard Security Gateways in your existing AWS infrastructure.

The Quick Start provides separate templates for these options. It also lets you configure CIDR blocks, instance types, and Check Point CloudGuard settings, as discussed later in this guide.

Deployment Steps

Step 1. Prepare Your AWS Account

1. If you don't already have an AWS account, create one at https://aws.amazon.com by following the on-screen instructions.
2. Use the region selector in the navigation bar to choose the AWS Region where you want to deploy Check Point CloudGuard Auto Scaling on AWS.
3. Create a key pair in your preferred region.
4. If necessary, request a service limit increase for the Amazon EC2 instance type you want to use for the Security Gateways, Security Management Server, and web servers. You might need to do this if you already have an existing deployment that uses these instance types, and you think you might exceed the default limit with this deployment. By default, this Quick Start uses **c5.xlarge** for the Security Gateways, **m5.xlarge** for the Security Management Server, and **t2.micro** for your workload of web servers.

Step 2. Subscribe to Check Point CloudGuard IaaS

1. Log in to AWS Marketplace at https://aws.amazon.com/marketplace.
2. Open the page for one of the following licensing options for Check Point CloudGuard Security Gateway:
   - CloudGuard IaaS Next-Gen Firewall w. Threat Prevention & SandBlast– BYOL

- CloudGuard IaaS Next-Gen Firewall with Threat Prevention – PAYG-NGTP
- CloudGuard IaaS Next-Gen Firewall with Threat Prevention and SandBlast – PAYG-NGTX

3. Choose **Continue to Subscribe**.
4. Choose **Accept Terms** to confirm your acceptance of the AWS Marketplace license agreement.
5. If you want to deploy a Check Point CloudGuard Security Management Server with this Quick Start, open the AWS Marketplace page for one of the following licensing options, and repeat steps 3 and 4:
   - CloudGuard IaaS Security Management – BYOL
   - CloudGuard IaaS Security Management for 25 Security Gateways – PAYG-MGMT

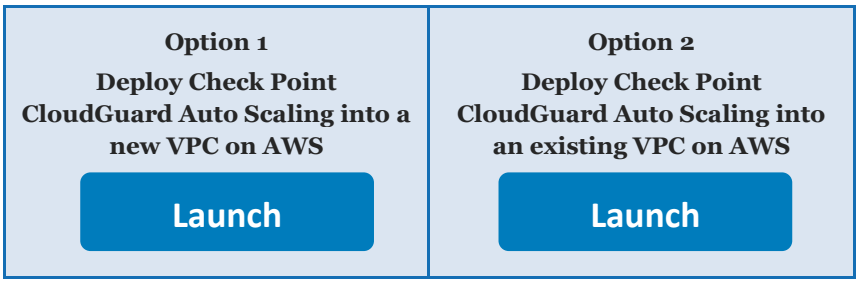
> **Note** If you want to manage more than 25 Security Gateways, either in the Auto Scaling group deployed by this Quick Start or in another environment, select the BYOL option and purchase a license. To purchase BYOL licenses, contact Check Point Sales.

When you deploy the Quick Start in the next step, you'll be prompted for the Security Gateway and Security Management Server licensing options you have selected.

Step 3. Launch the Quick Start

> **Note** You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using this Quick Start. For full details, see the pricing pages for each AWS service you will be using in this Quick Start. Prices are subject to change.

1. Choose one of the following options to launch the AWS CloudFormation template into your AWS account. For help choosing an option, see deployment options earlier in this guide.



> **Important** If you're deploying Check Point CloudGuard Auto Scaling into an existing VPC, make sure that your VPC has at least two public subnets in different Availability Zones for the Security Gateways, and two private subnets in different Availability Zones for your workload of web servers.

   Each deployment takes about 30 minutes to complete.

2. Check the region that's displayed in the upper-right corner of the navigation bar, and change it if necessary. This is where the network infrastructure for Check Point CloudGuard Auto Scaling will be built and where the resources will be deployed.
3. On the **Select Template** page, keep the default setting for the template URL, and then choose **Next**.
4. On the **Specify Details** page, change the stack name if needed. Review the parameters for the template. Provide values for the parameters that require input. For all other parameters, review the default settings and customize them as necessary. When you finish reviewing and customizing the parameters, choose **Next**.

   In the following tables, parameters are listed by category and described separately for the two deployment options:

   – Parameters for deploying Check Point CloudGuard Auto Scaling into a new VPC

   – Parameters for deploying Check Point CloudGuard Auto Scaling into an existing VPC

- **Option 1: Parameters for deploying Check Point CloudGuard Auto Scaling into a new VPC**

  View template

Network Configuration:

Parameter label (name)	Default	Description
VPC CIDR (VpcCidr)	10.0.0.0/16	The CIDR block for the VPC.
Availability Zones (AvailabilityZones)	*Requires input*	The specific Availability Zones you want to use for resource distribution. This field displays the available zones within your selected region. You can choose 2, 3, or 4 Availability Zones from this list. The logical order of your selections is preserved in your deployment. After you make your selections, make sure that the value of the **Number of Availability Zones** parameter matches the number of selections.
Number of AZs (NumberOfAZs)	2	The number of Availability Zones you want to use in your deployment, to ensure high availability of resources. You can specify 2, 3, or 4 Availability Zones. This count must match the number of selections you make from the **Availability Zones** parameter; otherwise, your deployment will fail with an AWS CloudFormation template validation error. (Note that some regions provide only 2 or 3 Availability Zones.)
Public Subnet 1 (PublicSubnetCidrA)	10.0.0.0/24	The CIDR block for the public (DMZ) subnet located in Availability Zone 1.
Public Subnet 2 (PublicSubnetCidrB)	10.0.2.0/24	The CIDR block for the public (DMZ) subnet located in Availability Zone 2.
Public Subnet 3 (PublicSubnetCidrC)	10.0.4.0/24	The CIDR block for the public (DMZ) subnet located in Availability Zone 3.
Public Subnet 4 (PublicSubnetCidrD)	10.0.6.0/24	The CIDR block for the public (DMZ) subnet located in Availability Zone 4.
Private Subnet 1 (PrivateSubnetCidrA)	10.0.1.0/24	The CIDR block for the private subnet located in Availability Zone 1.
Private Subnet 2 (PrivateSubnetCidrB)	10.0.3.0/24	The CIDR block for the private subnet located in Availability Zone 2.
Private Subnet 3 (PrivateSubnetCidrC)	10.0.5.0/24	The CIDR block for the private subnet located in Availability Zone 3.
Private Subnet 4 (PrivateSubnetCidrD)	10.0.7.0/24	The CIDR block for the private subnet located in Availability Zone 4.

General Settings:

Parameter label (name)	Default	Description
Key Name (KeyPairName)	*Requires input*	A public/private key pair, which allows you to connect securely to your instance after it launches. When you created an AWS

Parameter label (name)	Default	Description
		account, this is the key pair you created in your preferred region.
Auto Provision tag (Tag)	QuickStart	The tag used by the Security Management Server to automatically provision the Security Gateways. This is a string consisting of 1-12 alphanumeric characters and must be unique for each Quick Start deployment.
Email address (AdminEmail)	*Optional*	The email address that notifications about scaling events should be sent to.
Allow upload & download (AllowUploadDownload)	No	Set this parameter to **Yes** if you want to automatically download Software Blade Contracts and other important data. You can improve your experience with the product by sending data to Check Point. Visit the Check Point Cloud Services page for more information.
External Load Balancer (ExternalLoadBalancer Type)	Network Load Balancer	The type of external load balancer to use. Choose Network Load Balancer if you want to preserve the source IP address, or Application Load Balancer if you want to perform SSL offloading.
Protocol (Protocol)	HTTP	The protocol to use (HTTP or HTTPS).
HTTPS certificate (Certificate)	*Optional*	The Amazon Resource Name (ARN) of an HTTPS certificate. This field is ignored if the selected protocol is HTTP.
Custom service port (ServicePort)	*Optional*	The port that the external load balancer listens to. This is a number between 0 and 65535. Leave this field blank to use default ports: 80 for HTTP and 443 for HTTPS.

Check Point CloudGuard IaaS Security Gateways Auto Scaling Group Configuration:

Parameter label (name)	Default	Description
Instance type (GatewaysInstanceType)	c5.xlarge	The EC2 instance type for the Security Gateways.
Minimum group size (GatewaysMinSize)	2	The minimum number of Security Gateway instances in the Auto Scaling group.
Maximum group size (GatewaysMaxSize)	5	The maximum number of Security Gateway instances in the Auto Scaling group.
License (GatewaysLicense)	R80.30-PAYG-NGTX	The license to use for the Security Gateways. For an explanation of licensing options, see step 2. You must have a subscription to the corresponding AMI in AWS Marketplace.
Password hash (GatewaysPassword Hash)	*Optional*	The administrator user's password hash. You can use the following command to get this value: `openssl passwd -1` *password* For more information, see the Password hash section.

Parameter label (name)	Default	Description
SIC key (GatewaysSIC)	*Requires input*	The secure internal communication (SIC) key, which creates trusted connections between Check Point components. Choose a random string consisting of at least 8 alphanumeric characters. For more information, see the SIC key section.

Check Point CloudGuard IaaS Security Management Server Configuration:

Parameter label (name)	Default	Description
Deploy Management Server (ManagementDeploy)	Yes	Set this parameter to **No** if you want to use an existing Security Management Server or deploy one later. If you choose **No**, the Quick Start will ignore the other parameters in this section.
Instance type (ManagementInstance Type)	m5.xlarge	The EC2 instance type for the Security Management Server.
License (ManagementLicense)	R80.30-PAYG-MGMT	The license to use for the Security Management Server. For an explanation of licensing options, see step 2. You must have a subscription to the corresponding AMI in AWS Marketplace.
Password hash (ManagementPassword Hash)	*Optional*	The administrator user's password hash. You can use the following command to get this value: `openssl passwd -1` *password* For more information, see the Password hash section.
Security Policy (GatewaysPolicy)	Standard	The name of the security policy package to be installed on the gateways in the Auto Scaling group. For more information, see the Security Policy section.
Default Blades (GatewaysBlades)	On	Set this parameter to **Off** to disable the Intrusion Prevention System, Application Control, Antivirus, and Anti-Bot Software Blades. (These and additional blades can also be turned on or off manually after deployment.) For more information, see the Software Blades section.
Administrator addresses (AdminAddressCIDR)	*Requires input*	Allow web, SSH, and graphical clients only from this network to communicate with the Security Management Server
Gateways addresses (GatewaysAddresses)	10.0.0.0/16	The CIDR IP range that is permitted to access the Security Management Server. Only gateways from this network can communicate with the Security Management Server.

Web Servers Auto Scaling Group Configuration:

Parameter label (name)	Default	Description
Deploy Servers (ServersDeploy)	No	Set this parameter to **Yes** to deploy web servers and an internal Application Load Balancer. If you choose **No**, the Quick Start will ignore the other parameters in this section.
Instance type (ServersInstanceType)	t2.micro	The EC2 instance type for the web servers.
AMI ID (ServersAMI)	*Requires input*	The Amazon Machine Image (AMI) ID of the preconfigured web server to deploy (e.g. ami-0dc7dc63).

AWS Quick Start Configuration:

Parameter label (name)	Default	Description
Quick Start S3 Bucket Name (QSS3BucketName)	aws-quickstart	The S3 bucket you have created for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. The bucket name can include numbers, lowercase letters, uppercase letters, and hyphens, but should not start or end with a hyphen.
Quick Start S3 Key Prefix (QSS3KeyPrefix)	quickstart-checkpoint-autoscale/	The S3 key name prefix used to simulate a folder for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. This prefix can include numbers, lowercase letters, uppercase letters, hyphens, and forward slashes.

- **Option 2: Parameters for deploying Check Point CloudGuard Auto Scaling into an existing VPC**

View template

Network Configuration:

Parameter label (name)	Default	Description
VPC (VPC)	*Requires input*	The ID of your existing VPC (e.g., vpc-0343606e).
Key Name (KeyPairName)	*Requires input*	A public/private key pair, which allows you to connect securely to your instance after it launches. When you created an AWS account, this is the key pair you created in your preferred region.
Auto Provision tag (Tag)	QuickStart	The tag used by the Security Management Server to automatically provision the Security Gateways. This is a string

Parameter label (name)	Default	Description
		consisting of 1-12 alphanumeric characters and must be unique for each Quick Start deployment.
Email address (AdminEmail)	*Optional*	The email address that notifications about scaling events should be sent to.
Allow upload & download (AllowUploadDownload)	No	Set this parameter to **Yes** if you want to automatically download Software Blade Contracts and other important data. You can improve your experience with the product by sending data to Check Point. Visit the Check Point Cloud Services page for more information.
External Load Balancer (ExternalLoadBalancer Type)	Network Load Balancer	The type of external load balancer to use. Choose Network Load Balancer if you want to preserve the source IP address, or Application Load Balancer if you want to perform SSL offloading.
Protocol (Protocol)	HTTP	The protocol to use (HTTP or HTTPS).
HTTPS certificate (Certificate)	*Optional*	The Amazon Resource Name (ARN) of an HTTPS certificate. This field is ignored if the selected protocol is HTTP.
Custom service port (ServicePort)	*Optional*	The port that the external load balancer listens to. This is a number between 0 and 65535. Leave this field blank to use default ports: 80 for HTTP and 443 for HTTPS.

Check Point CloudGuard IaaS Security Gateways Auto Scaling Group Configuration:

Parameter label (name)	Default	Description
Subnets (GatewaySubnets)	Requires input	The IDs of the public subnets to use for the Security Gateways. Specify at least two subnets, separated by commas, from your existing VPC (for example, subnet-0d72417c,subnet-1f61306f,subnet-1061d06f). If you choose to include a Security Management Server, it will be deployed in the first subnet.
Instance type (GatewaysInstanceType)	c5.xlarge	The EC2 instance type for the Security Gateways.
Minimum group size (GatewaysMinSize)	2	The minimum number of Security Gateway instances in the Auto Scaling group.
Maximum group size (GatewaysMaxSize)	5	The maximum number of Security Gateway instances in the Auto Scaling group.
License (GatewaysLicense)	R80.30-PAYG-NGTX	The license to use for the Security Gateways. For an explanation of licensing options, see step 2. You must have a subscription to the corresponding AMI in AWS Marketplace.
Password hash (GatewaysPassword Hash)	*Optional*	The administrator user's password hash. You can use the following command to get this value:

		`openssl passwd -1` *password* For more information, see the Password hash section.
SIC key (GatewaysSIC)	*Requires input*	The secure internal communication (SIC) key, which creates trusted connections between Check Point components. Choose a random string consisting of at least 8 alphanumeric characters. For more information, see the SIC key section.

Check Point CloudGuard IaaS Security Management Server Configuration:

Parameter label (name)	Default	Description
Deploy Management Server (ManagementDeploy)	Yes	Set this parameter to **No** if you want to use an existing Security Management Server or deploy one later. If you choose **No**, the Quick Start will ignore the other parameters in this section.
Instance type (ManagementInstance Type)	m5.xlarge	The EC2 instance type for the Security Management Server.
License (ManagementLicense)	R80.30-PAYG-MGMT	The license to use for the Security Management Server. For an explanation of licensing options, see step 2. You must have a subscription to the corresponding AMI in AWS Marketplace.
Password hash (ManagementPassword Hash)	*Optional*	The administrator user's password hash. You can use the following command to get this value: `openssl passwd -1` *password* For more information, see the Password hash section.
Security Policy (GatewaysPolicy)	Standard	The name of the security policy package to be installed on the gateways in the Auto Scaling group. For more information, see the Security Policy section.
Default Blades (GatewaysBlades)	On	Set this parameter to **Off** to disable the Intrusion Prevention System, Application Control, Antivirus, and Anti-Bot Software Blades. (These and additional blades can also be turned on or off manually after deployment.) For more information, see the Software Blades section.
Administrator addresses (AdminAddressCIDR)	*Requires input*	Allow web, SSH, and graphical clients only from this network to communicate with the Security Management Server.
Gateways addresses (GatewaysAddresses)	10.0.0.0/16	The CIDR IP range that is permitted to access the Security Management Server. Only gateways from this network can communicate with the Security Management Server.

Web Servers Auto Scaling Group Configuration:

Parameter label (name)	Default	Description
Deploy Servers (ServersDeploy)	No	Set this parameter to **Yes** to deploy web servers and an internal Application Load Balancer. If you choose **No**, the Quick Start will ignore the other parameters in this section.
Subnet IDs (ServersSubnets)	*Requires input*	The IDs of the private subnets to use for the web servers. Specify at least two subnets, separated by commas, from your existing VPC (for example, subnet-0d72417c,subnet-1f61306f,subnet-1061d06f). If you choose to include a Security Management Server, it will be deployed in the first subnet.
Instance type (ServersInstanceType)	t2.micro	The EC2 instance type for the web servers.
AMI ID (ServersAMI)	*Requires input*	The Amazon Machine Image (AMI) ID of the preconfigured web server to deploy (e.g. ami-0dc7dc63).

5. On the **Options** page, you can specify tags (key-value pairs) for resources in your stack and set advanced options. When you're done, choose **Next**.
6. On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the check box to acknowledge that the template will create IAM resources.
7. Choose **Create** to deploy the stack.
8. Monitor the status of the stack. When the status is **CREATE_COMPLETE**, the Check Point CloudGuard Auto Scaling stack is ready.
9. Use the following values displayed in the **Outputs** tab if you want to configure the environment further:

Key	Description
ALBURL	If you have chosen to deploy an Application Load Balancer, this value is its DNS name.
NLBURL	If you have chosen to deploy a Network Load Balancer, this value is its DNS name.
ControllerName	The name that represents the controller. Configurations required for the Security Management Server to connect to your AWS environment in order to automatically provision the Security Gateways, such as credentials and the region, will be placed under this controller name.
ManagementName	The name that represents the Security Management Server. This name is used to deploy the Auto Scaling group, so it will be identified and automatically provisioned by the Security Management Server. This name is also used to tag

Key	Description
	the internal load balancer so that it can be recognized and traffic can be forwarded to it.
ConfigurationTemplateName	Configurations required to automatically provision the Security Gateways in the Auto Scaling group, such as which policy to install and Software Blades to enable, will be placed under this template name. This name is used to deploy the Auto Scaling group as a reference to the relevant set of configurations to apply on the group and to tag the internal load balancer. You can use different templates to maintain multiple sets of configurations to associate with different Auto Scaling groups managed by a single Security Management Server.
InternalPort	If you intend to manually deploy your Auto Scaling group of web servers, the internal load balancer should listen to this port.

The following sections provide additional information about parameter settings.

Password hash

To manage the environment's security, administrators can connect to the Security Management Server with SmartConsole clients and to Check Point instances via the Gaia WebUI.

When you deploy the Quick Start, you can set the administrator password for CloudGuard Security Management Server and Security Gateways by using the two **Password hash** parameters. To protect the password, you must provide the password's MD5-based BSD password algorithm 1 salted hash instead of the password itself.

You can pre-generate the password's salted hash with the following command:

```
openssl passwd -1 password
```

Security policy

A security policy package is a collection of different types of policies that are enforced after the policy is installed on the Security Gateways. A policy package can have one or more of these policy types: Access Control, Quality of Service (QoS), Desktop Security, and Threat Prevention.

If you select to deploy a Check Point Security Management Server with this Quick Start, you can specify the name of the security policy package to be installed on the gateways by using the **Security Policy** parameter. The default name is **Standard**.

The **Standard** policy package is the default security policy defined in a newly deployed Security Management Server, and initially contains a default cleanup rule that drops all traffic. If you intend to configure additional policy packages (for example, if you plan to manage the security of additional environments protected by Check Point's products) and want to install a different policy package on the Security Gateways deployed by this Quick Start, specify the name you want to give that policy package in the **Security Policy** field. Then, create and configure the policy by connecting to your Security Management Server with SmartConsole.

This Quick Start preconfigures the deployed Security Management Server to create, in the policy package you have specified, the necessary NAT and access control rules to enable traffic flow from the Security Gateways to your web servers and back.

SIC key

The secure internal communication (SIC) key creates trusted connections between Security Gateways, Security Management Servers, and other Check Point components. Trust is required to install policies on the Security Gateways and to send logs from the Security Gateways to Security Management Servers.

Select a random string consisting of at least 8 alphanumeric characters and specify it in the **SIC key** parameter during deployment. If you choose to use a manually configured Security Management Server to manage the Auto Scaling group of Security Gateways deployed by this Quick Start, the SIC key is necessary to complete the configuration of the Security Management Server.

Software Blades

A Software Blade is a security application or module such as Firewall, Intrusion Prevention System (IPS), or Application Control, which is independent, modular, and centrally managed.

The CloudGuard Security Gateways are preconfigured with the Firewall Blade enabled. Additionally, this Quick Start enables, by default, the Intrusion Prevention System, Application Control, Antivirus, and Anti-Bot Blades. To disable these blades, you can set the **Default Blade** parameter to **No**. To enable additional Software Blades or disable active ones after deployment, see the section Enabling and disabling Software Blades in Check Point's *Security Management Server with CloudGuard for AWS* documentation.

Step 4. Review and Test the Deployment

1. Review the deployment in the AWS Management Console. A working setup will include the following:
    - An Auto Scaling group of Check Point CloudGuard Security Gateways.
    - An external Application or Network Load Balancer that will route traffic to the Auto Scaling group of Security Gateways.
    - An Auto Scaling group of configured web servers that run at the service port.
    - An internal Application Load Balancer that will route traffic to the Auto Scaling group of web servers, and receive traffic from the Auto Scaling group of Security Gateways.
    - A Check Point Security Management Server deployed either on AWS or on premises and configured to automatically provision the Auto Scaling group of CloudGuard Security Gateways.

2. To test the deployment, verify that the protected web service is accessible via the external Application or Network Load Balancer DNS address, as specified in the CloudFormation stack **Outputs** tab.

> **Important** If you choose to manually deploy and configure the Security Management Server or the Auto Scaling group of web servers and its internal load balancer, the environment will not be functional until you do so. This means that the Security Gateway instances will appear unhealthy and the external load balancer DNS address will return an error message.

Check Point Security Management Server

The CloudGuard Security Gateways are automatically managed by a Check Point Security Management Server that can be deployed either on AWS or on premises.

During scale-out events, in which new Security Gateway instances are launched to meet an increase in current load, the Security Management Server performs the necessary configuration of the Security Gateways and security policies to facilitate the inspection and routing of traffic.

During scale-in events, in which existing Security Gateway instances are terminated as a result of a decrease in current load, the Management Server cleans up any settings that were created when the Security Gateways were launched.

For more information about scale-out and scale-in, see Check Point's CloudGuard Auto Scaling in AWS documentation.

If you have chosen to deploy a Check Point Security Management Server with this Quick Start by accepting the default setting of the **Deploy Management Server** parameter, it is deployed and configured to automatically provision the Security Gateways so they will inspect and route traffic to the workload of web servers placed behind them. The IAM policy that will be attached to the Security Management Server's IAM role will enable it to read Amazon EC2, Elastic Load Balancing, and Auto Scaling properties.

If you set the **Deploy Management Server** parameter to **No**, you can either use an existing Management Server or deploy one later.

To manually deploy and configure a CloudGuard Security Management Server, either on AWS or on premises, see the section Installing and configuring the Check Point Security Management Server in Check Point's *CloudGuard Auto Scaling for AWS* documentation.

The CloudFormation stack **Outputs** tab specifies the tags and values with which the resources were deployed. You may use this information if you are configuring the Auto Provisioning service for the first time.

> **Important** If you are configuring the Security Management Server manually, make sure that the values for the management name and the configuration template name in the Management Server configuration match the tags and values of the load balancers and the Auto Scaling group of Security Gateways.

For advanced configuration, such as enabling and disabling Software Blades, see Check Point's Security Management Server with CloudGuard for AWS documentation.

Web Servers Workload

If you have chosen to deploy a workload of web servers with this Quick Start by setting the **Deploy Servers** parameter to **Yes**, an internal Application Load Balancer will also be deployed to route traffic to the workload from the Security Gateways. The Auto Scaling settings of the web servers, such as the minimum and maximum group sizes, will match those of the Auto Scaling group of Security Gateways, as specified by the **Minimum Group Size** and **Maximum Group Size** parameters during deployment. These settings can be modified from the **Auto Scaling Groups** tab in the AWS Management Console.

The Auto Scaling group of CloudGuard Security Gateways will be automatically provisioned by the Security Management Server so that the Security Gateways will forward the inspected traffic to the internal Application Load Balancer.

To use this Quick Start to protect an existing workload of web servers, see the FAQ section.

The Shared Responsibility Model

To fully embrace the cloud, businesses need to understand the balance of responsibilities between protecting the cloud infrastructure (which is the cloud provider's responsibility) and protecting the data that resides in the cloud (which is the customer's responsibility).

For more information about the shared responsibility model, visit the AWS Shared Responsibility Model page and Check Point's whitepaper about protecting critical assets in public clouds.

FAQ

Q. I encountered a CREATE_FAILED error when I launched the Quick Start.

A. If AWS CloudFormation fails to create the stack, we recommend that you relaunch the template with **Rollback on failure** set to **No**. (This setting is under **Advanced** in the AWS CloudFormation console, **Options** page.) With this setting, the stack's state will be retained and the created instances will be left running, so you can troubleshoot the issue.

> **Important** When you set **Rollback on failure** to **No**, you will continue to incur AWS charges for this stack. Please make sure to delete the stack when you finish troubleshooting.

For additional information, see Troubleshooting AWS CloudFormation on the AWS website.

Q. How can I use this Quick Start to protect an existing workload of web servers?

A. You can place an existing workload of web servers, or manually deploy a new workload, behind the CloudGuard Auto Scaling group of Security Gateways. To do so, follow these steps:

1. Select **No** for the **Deploy Servers** parameter when launching the Quick Start.
2. Place the web server workload in private subnets.
3. Create an internal load balancer that listens to the internal port, as specified in the CloudFormation stack **Outputs** tab.
4. Attach the load balancer's target group to the web server workload.
5. Tag the internal load balancer as described in the section Adding tags to your Internal Elastic Load Balancer in Check Point's *CloudGuard Auto Scaling for AWS* documentation. The values required to complete this step are described in the CloudFormation stack **Outputs** tab, if you have chosen to deploy a Security Management Server using this Quick Start. Otherwise, you can determine these values when you configure the Management Server, as described in the section Installing and configuring the Check Point Security Management Server in Check Point's *CloudGuard Auto Scaling for AWS* documentation.

> **Tip** It is also possible to have the web servers workload deployed in a different AWS account. See the section Connecting with Additional AWS accounts in Check Point's *Security Management Server with CloudGuard for AWS* documentation.

Q. How do I manually deploy a Check Point Security Management Server to manage the CloudGuard Security Gateways?

A. Choose **No** for the **Deploy Management Server** parameter during deployment (step 3), and follow the steps described in the Check Point Security Management Server section.

Q. How do I configure an existing Check Point Security Management Server to manage the CloudGuard Security Gateways?

A. Choose **No** for the **Deploy Management Server** parameter during deployment (step 3), and follow the steps described in the Check Point Security Management Server section.

Q. How do I enable additional Software Blades or disable active ones?

A. See the section Enabling and disabling Software Blades in Check Point's *Security Management Server with CloudGuard for AWS* documentation.

Git Repository

You can visit our GitHub repository to download the templates and scripts for this Quick Start, to post your comments, and to share your customizations with others.

Additional Resources

AWS services

- Amazon EBS
  https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html
- Amazon EC2
  https://aws.amazon.com/documentation/ec2/
- Amazon VPC
  https://aws.amazon.com/documentation/vpc/
- AWS CloudFormation
  https://aws.amazon.com/documentation/cloudformation/
- AWS Auto Scaling
  https://aws.amazon.com/ec2/autoscaling/
- AWS Identity and Access Management (IAM)
  https://aws.amazon.com/iam/

- Amazon Simple Notification Service (SNS)
  https://aws.amazon.com/sns/

Check Point CloudGuard IaaS

- CloudGuard Auto Scaling for AWS
  https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk112575
- Security Management Server with CloudGuard for AWS

  https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk130372
- AWS CloudFormation Templates
  https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk111013
- Configuration of AWS STS to Delegate Access across two AWS accounts
  https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk122074
- Secure Cloud Blueprint: Agile Security Architecture for the Cloud
  https://pages.checkpoint.com/secure-cloud-blueprint.html

Quick Start reference deployments

- AWS Quick Start home page
  https://aws.amazon.com/quickstart/

Document Revisions

Date	Change	In sections
September 2019	Updated license links	Step 2
July 2019	Updated AMI name; increased number of Security Gateways	Steps 2 and 3
June 2018	Initial publication	—

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

The software included with this paper is licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at http://aws.amazon.com/apache2.0/ or in the "license" file accompanying this file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.