Check Point
SOFTWARE TECHNOLOGIES LTD.

12 July 2021

TRANSIT VPC FOR AWS

R80.10

CloudGuard IaaS for AWS Transit VPC

Deployment Guide

Classification: [Protected]

STEP UP TO
5TH GENERATION
CYBER SECURITY

2021 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page https://www.checkpoint.com/copyright/ for a list of our trademarks.

Refer to the Third Party copyright notices https://www.checkpoint.com/about-us/third-party-trademarks-and-copyrights/ for a list of relevant copyrights and third-party licenses.

Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page https://www.checkpoint.com/products-solutions/certified-check-point-solutions/.

Latest Version of this Document

Open the latest version of this document in a Web browser https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_Transit_VPC_for_AWS/html_frameset.htm.

Download the latest version of this document in PDF format http://downloads.checkpoint.com/dc/download.htm?ID=67724.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Transit VPC for AWS R80.10 Deployment Guide.

Revision History

Date	Description
12 July 2021	Added the note that Transit VPC is a deprecated solution and the link to **sk153473**.
11 October 2018	• Improved procedures and explanations • Updated: Use Cases (on page 10) - added "Direct Connect"
26 December 2018	Updated: Limitations (on page 46) - Added support for R80.10 Jumbo Hotfix Accumulator Take 142 (or above)
11 July 2018	First release of this document

Contents

Important Information....3
Terms....5
Overview....7
AWS Global Transit Network and CloudGuard....7
Solution Highlights for Check Point CloudGuard IaaS for AWS....8
Costs and Licenses....8
Prerequisites....9
Architecture....9
Use Cases....10
VPN Community....10
Security Policy....11
Deployments Options....12
Deployment Steps....13
Step 1: Preparing Your AWS Account....13
Step 2: Subscribing to Check Point CloudGuard IaaS....14
Step 3: Deploying Security Transit VPC....15
Parameters for Deploying Security Transit into a New VPC....16
Parameters for Deploying Security Transit into an Existing VPC....19
Configuring the Environment after the Deployment....21
Step 4: Reviewing and Testing the Deployment....22
Check Point CloudFormation Templates....23
Template Parameters....23
Parameter Description....23
Additional Features....24
Configuring VPN between the Transit CloudGuard Gateways and Your On-Premises Gateway....24
Tagging a Spoke VPC....25
Setting a Role on a Spoke VPC Account....25
Multi-Hub Support....26
Exporting Custom Routes to Spokes....27
Enabling Custom Routes to Spokes....28
Ignore Manually Created VPN Connections....29
Ignore Manually Created Customer Gateways....29
Changing the ASN of the Transit Gateway....30
Running Transit and Auto-Scaling Simultaneously....31
Deploying a Security Management Server Without an Internet Connection....32
Advanced Configuration....33
Deploying and Configuring the Check Point Security Management Server....33
Required Permissions for the Security Management Server....33
Deploying the Security Management Server....34
Configuring the Security Management Server....35
Configuring the Multi-Domain Server....40
Troubleshooting....41
Limitations....46
Additional Resources....47

Terms

Amazon EC2

Amazon Elastic Compute Cloud. A service for running and maintaining a specified number of tasks simultaneously (definition from AWS glossary).

Anti-Bot

1. An application that prevents computers from being controlled by hackers.

2. Check Point Software Blade that inspects network traffic for malicious bot software.

Anti-Virus

A solution to protect a computer or network against self-propagating programs or processes that can cause damage.

AWS CloudFormation

A service for writing or changing templates that creates or deletes related AWS resources together as a unit (definition from AWS glossary).

AWS IAM

AWS Identity and Access Management. A web service that enables AWS customers to manage users and user permissions within AWS (definition from AWS glossary).

AWS VPC

AWS Virtual Private Cloud. A private cloud that exists in the public cloud of Amazon. It is isolated from other Virtual Networks in the AWS cloud.

Expert Mode

The name of the full command line shell that gives full system root permissions in the Check Point Gaia operating system.

Warning - Expert Mode should be used with caution. The flexibility of an open shell, with root permission, exposes the system to the possibility of administrative errors.

Hub-and-Spoke Network Topology

A virtual private network community with gateways defined as spokes that create tunnels only with the central gateway (hub).

Instance

A copy of an Amazon Machine Image (AMI) running as a virtual server in the AWS cloud (definition from AWS glossary).

IPS

Intrusion Prevention System. Check Point Software Blade that inspects and analyzes packets and data for numerous types of risks.

IPSec

A security protocol for authentication and encryption over the Internet.

Software Blade

A software blade is a security solution based on specific business needs.

Each blade is independent, modular and centrally managed. To extend security, additional blades can be quickly added.

STS Role

AWS Security Token Service. A web service for requesting temporary, limited-privilege credentials for IAM users or for users that you authenticate (definition from AWS glossary).

Subnet

A segment of the IP addresses range of a VPC, to which EC2 instances are attached. EC2 instances are grouped into subnets based on security and operational needs (definition from the AWS glossary).

VTI

Virtual Tunnel Interface. A virtual interface that is a member of an existing, Route Based, VPN tunnel.

Zero-Day Attack

Also Zero-Hour attack. An exploit that targets publicly known but still unpatched vulnerabilities, for which security developers

can counter and publish a solution within the hour or day.

Overview

In This Section:

AWS Global Transit Network and CloudGuard 7
Solution Highlights for Check Point CloudGuard IaaS for AWS....8
Costs and Licenses....8
Prerequisites 9
Architecture 9
Use Cases....10
VPN Community....10
Security Policy 11
Deployments Options 12

AWS Global Transit Network and CloudGuard

Important - Transit VPC is a deprecated solution. Refer to sk153473 - How to migrate from Transit VPC to AWS Transit Gateway https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk153473.

The Amazon Global Transit Network is used to perform transitive routing between spoke networks through a central hub. Use this document to deploy a hub-and-spoke network topology that routes all traffic through a network transit center, a Transit VPC.

The Transit VPC simplifies network management and minimizes the number of connections needed to connect multiple Amazon VPCs and remote networks. You can create as many virtual networks as necessary and design different options for connecting the networks to each other.

Use Check Point CloudGuard together with the Transit VPC. CloudGuard delivers comprehensive security for cloud workloads and assets with VPC perimeter security services, seamless security segmentation between VPCs, and automatically established IPsec VPN connectivity between cloud environments. The solution automatically connects spoke VPCs to a central security hub VPC for seamless security inspection, VPN and NAT services.

CloudGuard integrates easily with AWS. Once you deploy the Security Management Server and security hub, every new or existing VPC that is specifically tagged is automatically configured to route all traffic. The traffic is routed through an AWS managed VPN gateway into the security hub. The VPN gateways are also added as IPsec interoperable devices. The Security Gateways are added to the automatically established route-based VPN process, (powered by Border Gateway Protocol (BGP)), to propagate network route changes to on-premises and in cloud tenants.

The solution provides the Check Point award winning Threat Prevention suite in transit architecture. It offers industry leading Firewall (according to NSS and Gartner), IPS, HTTPS Inspection, Anti-Bot and Anti-Virus, and Zero-day protection engines. These Threat Prevention features safeguard published applications, Internet-bound traffic, and inbound access to cloud assets with complete security visibility and event analysis.

Solution Highlights for Check Point CloudGuard IaaS for AWS

Check Point CloudGuard for AWS easily extends comprehensive Threat Prevention security to the AWS cloud and protects assets in the cloud from attacks, and at the same time enables secure connectivity.

CloudGuard IaaS lets you enforce consistent Security Policies across your entire organization. It protects data between the corporate network and the Amazon VPC. CloudGuard IaaS also inspects data that enters and leaves the private subnet in the Amazon VPC to prevent attacks and mitigate data loss or leakage. CloudGuard IaaS protects services in the public cloud from the most sophisticated threats as well as unauthorized access, and at the same time prevents application layer Denial of Service (DoS) attacks.

Check Point CloudGuard for AWS meets organizational cloud security needs:

- Automatically deployed tags-based IPsec VPN between spoke VPCs and the security hub VPC.
- Automatic configuration of AWS VPN Gateways on spoke VPCs. This includes IP address planning to avoid subnet IP address conflicts.
- Next Gen Firewall including Application Control, Data Awareness, HTTPS Inspection, NAT, and logging.
- IPS and virtual patching of cloud resources.
- URL Filtering for Internet-bound traffic.
- Anti-Bot and Anti-Virus, and Zero-day Threat Emulation and Threat Extraction.
- Remote Access VPN to connect remote clients.
- IPsec VPN for VPC-to-VPC, and VPC-to-on-premises connections with optional Direct Connect support.
- High Availability deployment.
- Automated solution deployment using CloudFormation.

Costs and Licenses

You are responsible for the cost of the AWS services that you use, when you deploy the solution described in this guide.

The AWS CloudFormation template for the Transit VPC includes configuration parameters that you can customize. Some of these settings, such as instance type, affect the cost of deployment. For estimated costs, see the AWS pricing calculator.

This Transit VPC solution uses Amazon Machine Images (AMIs) from the AWS Marketplace. You must subscribe to Check Point CloudGuard in the AWS Marketplace before you start the deployment.

You need a license to use the Check Point CloudGuard Security Gateways, Check Point CloudGuard Security Management Server, and AWS CloudFormation templates described in this guide. There are two licensing options:

- Pay As You Go (PAYG)
- Bring Your Own License (BYOL)

To purchase BYOL licenses, contact Check Point Sales.

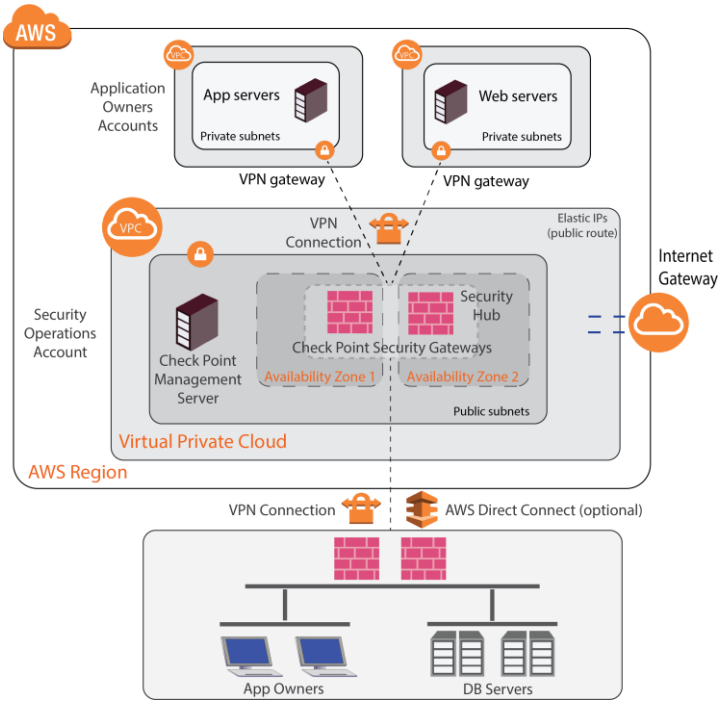
Prerequisites

Before you use this solution, make sure you are familiar with these AWS services:

- Amazon EC2
- Amazon VPC
- AWS CloudFormation
- AWS IAM

If you are new to AWS, see *Getting Started with AWS* https://aws.amazon.com/getting-started/.

Architecture



The diagram shows the end-to-end solution, which includes:

- Check Point Security Management Server deployed in AWS.
- Transit VPC (Hub VPC) with two Check Point CloudGuard IaaS Security Gateways in two different AWS Availability Zones for High Availability.
- Spoke (Consumer) VPCs with AWS virtual gateways, automatically provisioned when they are tagged.
- Automatic provisioning of VPN tunnels and BGP routing configuration between the spoke VPCs and the CloudGuard IaaS Security Gateways.
- Configuration of the BGP routing between the on-premises perimeter gateway and the CloudGuard IaaS Security Gateways.

Use Cases

These are the examples of how you can set up your Transit VPC architecture:

Architecture	Description
Transparent proxy	The transparent proxy provides secured proxy services to the spoke VPCs. It is transparent in that the security proxy services are seamless and do not require topological changes to the protected spoke VPCs. With this solution, you do not need a CloudGuard Gateway for AWS in each of the spoke VPCs. The solution relies on VPN connections to the central (hub) VPC for Internet-bound connections. DevOps and application owners can use the transparent proxy to deploy solutions in designated VPCs, rely on AWS native security controls only, and have advanced Threat Prevention, Next Generation Firewall, and compliance, seamlessly from the central VPC.
Cloud perimeter	The Transit VPC, as a cloud perimeter, provides Threat Prevention and Access Control to the spoke VPCs. Each VPC can be deployed in multiple Availability Zones and provide security services to multiple spoke VPCs in the environment. Only the central VPC has access to the Internet, and the spokes are limited to private subnets. All traffic to and from the spoke VPCs is steered through the central VPC. The security controls are concentrated in a single central VPC.
Hybrid cloud	With a Hybrid cloud setup, you can connect your on-premises and cloud environments, and cloud assets can have secured access to on-premises assets. The connection is established through a secured VPN connection between your Check Point Security Gateway and a CloudGuard Gateway in AWS. You can also implement a secure connection with AWS Direct Connect tunnels. For example, a front-end server in the cloud can connect to an on-premises backend database to retrieve confidential data or business logic. For more information, see sk120534. http://supportcontent.checkpoint.com/solutions?id=sk120534
Direct Connect	Direct Connect makes it easy to establish a dedicated network connection from on-premises to AWS. When you use AWS Direct Connect, it is transparent to Check Point Security Gateways. For example, you can connect route and tunnels from Transit Gateways directly to corporate gateways. You must configure the Direct Connect manually, when you connect corporate gateways and Transit Gateways. Automation is not supported. For more information, see sk120534 http://supportcontent.checkpoint.com/solutions?id=sk120534.

VPN Community

A VPN Domain is a collection of internal networks that use VPN Security Gateways to send and receive their traffic. VPN Security Gateways are joined into a VPN Community. A VPN Community is a collection of VPN tunnels and their attributes. Networks from different VPN Domains can

communicate securely with each other through VPN tunnels that terminate at the Security Gateways in the VPN communities.

VPN communities used for this Transit solution are based on a Star topology. In a Star VPN Community, each satellite gateway, an AWS VPN connection represented by an Interoperable Device object, has a VPN tunnel to the central CloudGuard Security Gateway, and through it to other satellite gateways in the Star VPN Community.

Transit solution uses Route Based VPN, where VPN traffic is routed based on the BGP routing settings of the CloudGuard Gateway. The CloudGuard Gateway uses a VPN Tunnel Interface (VTI) to send the VPN traffic, as if it were a physical interface.

Because of the Route Based VPN, there is no need to set a VPN Domain on the CloudGuard Security Gateway. The Transit service creates an empty Group object that is used when you configure the CloudGuard Gateway in SmartConsole. This ensures that Domain Based VPN is not used.

The `config-community.sh` script creates a Star VPN Community with these required settings for Transit:

- Encryption: IKE Security Association Phase 2 enabled, set to Group 2 (1024 bit)
- Tunnel management: **One VPN tunnel per gateway pair** enabled
- Shared Secret: **Use only Shared Secret for all external members** enabled
- Advanced: IKE (Phase 1) set to 480

For information on this script, see the *Configuring the VPN Community with the 'config-community.sh' Script* (on page 38) section.

For more information on Check Point VPN solutions, see the *R80.10 Site to Site VPN Administration Guide* https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_SitetoSiteVPN_AdminGuide/html_frameset.htm.

Security Policy

A Security Policy package is a collection of different types of policies that are enforced after you install the policy on the Security Gateways.

A policy package can have one or more of these policy types:

- Access Control
- Quality of Service (QoS)
- Desktop Security
- Threat Prevention

The Standard policy package is the default Security Policy defined in a newly deployed Security Management Server. Every policy package contains a default cleanup rule that drops all traffic.

When you configure the <Check Point Security Management Server with the autoprov-cfg utility, specify the name of the Security Policy package to be installed on the Transit Gateways with the -po parameter. For the default Security Policy, use the value "Standard" (a capital "S" is required), for this parameter.

If you want to configure additional policy packages and install a different policy package on the Security Gateways deployed for the transit solution, then specify the name that you want to give

that policy package when you run autoprov-cfg. Afterwards, create and configure the policy by connecting to your Security Management Server with SmartConsole.

For more information, see 'autprov-cfg (on page 35)'

Deployments Options

There are two deployment options:

Option	Description
Deploy the Check Point CloudGuard transit solution as a **new VPC**	This option builds a new AWS transit environment that consists of the VPC, subnets, security groups, and other infrastructure components. It then deploys the Check Point CloudGuard IaaS Security Gateways into this new VPC and an optional preconfigured Security Management Server to manage them.
Deploy the Check Point CloudGuard transit solution into an **existing VPC**	This option provisions Check Point CloudGuard IaaS Security Gateways and an optional preconfigured Security Management Server to manage them into your existing AWS infrastructure.

There are separate CloudFormation templates for each option. The templates let you configure CIDR blocks, instance types, and Check Point CloudGuard IaaS settings.

See Step 3 (on page 14) for links to the templates.

Deployment Steps

In This Section:

Step 1: Preparing Your AWS Account....13
Step 2: Subscribing to Check Point CloudGuard IaaS....13
Step 3: Deploying Security Transit VPC....14
Step 4: Reviewing and Testing the Deployment....21

Step 1: Preparing Your AWS Account

Step	Description
1	If you do not already have an AWS account, create one at AWS https://aws.amazon.com/getting-started/.
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 https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html in your preferred region.
4	If necessary, request a service limit increase for the AWS resources you are going to use. You may have to do this, if you have an existing deployment that uses the AWS resources below, and you may exceed the default limit with this deployment. The resources that may need a service limit increase are: • Number of On-demand EC2 instances. • Number of Elastic IP addresses. • Number of VPCs per region. • Number of VPN connections per region. • Number of virtual private gateways per region. • VPN connections per VPC.

By default, this Deployment guide uses **c4.xlarge** for the Security Gateways and **m4.xlarge** for the Security Management Server.

Step 2: Subscribing to Check Point CloudGuard IaaS

Step	Description
1	Log in to AWS Marketplace https://aws.amazon.com/marketplace.
2	Select one of these licensing options for Check Point CloudGuard Security Gateways: • CloudGuard IaaS Next Gen firewall and Threat Prevention (BYOL) https://aws.amazon.com/marketplace/pp/B07D77VMSJ • CloudGuard IaaS Next Gen firewall and Threat Prevention (PAYG-NGTP) https://aws.amazon.com/marketplace/pp/B07D783LJ9 • CloudGuard IaaS Next Gen firewall and Advanced Threat Prevention (PAYG-NGTX) https://aws.amazon.com/marketplace/pp/B076H63V1L
3	Select **Continue** to subscribe.
4	Select **Accept Terms** to confirm that you accept the AWS Marketplace license agreement.
5	If you want to deploy a Check Point CloudGuard Security Management Server, repeat Step 3 and Step 5 in this procedure and select one of these licensing options: • CloudGuard IaaS Security Management (BYOL) • CloudGuard IaaS Security Management for five Security Gateways (PAYG-MGMT5) **Note** - If you want to manage more than five Security Gateways, select the BYOL option to purchase a license. Contact Check Point Sales https://www.checkpoint.com/about-us/contact-us/ to purchase a license.

When you deploy the Transit VPC in the steps that follow, you are prompted for the licensing information for the Security Gateways and Security Management Server that you selected.

Step 3: Deploying Security Transit VPC

Select one of these options to launch the Transit VPC template into your AWS account:

Option	CloudFormation Template	Direct Link
Deploy Check Point CloudGuard IaaS Transit into a **new VPC on AWS**	New VPC	Launch new VPC https://console.aws.amazon.com/cloudformation/home?#/stacks/create/review?templateURL=https%3A%2F%2Fs3.amazonaws.com%2FCloudFormationTemplate%2Fcheckpoint-transit-master.yaml&stackName=Check-Point-Transit-VPC
Deploy Check Point CloudGuard IaaS Transit into an **existing VPC on AWS**	Existing VPC	Launch existing VPC https://console.aws.amazon.com/cloudformation/home?#/stacks/create/review?templateURL=https%3A%2F%2Fs3.amazonaws.com%2FCloudFormationTemplate%2Fcheckpoint-transit.yaml&stackName=Check-Point-Transit-VPC

Important - If you deploy Check Point CloudGuard IaaS Transit into an existing VPC, make sure that your VPC has:

- Two public subnets in different Availability Zones for the Security Gateways
- Two private subnets in different Availability Zones that will serve as the Security Gateway internal networks

Each deployment might take approximately 30 minutes to complete.

Parameters for Deploying Security Transit into a New VPC

General Settings:

Parameter name	Default	Description
VPC CIDR	10.0.0.0/16	Specifies the CIDR block for the VPC.
Availability Zones	Requires input	Specifies the Availability Zones you want to use for resource distribution. This field displays the available zones within your selected region. You must select two availability zones from this list. The logical order of your selections is preserved in your deployment.
Public Subnet 1	10.0.0.0/24	Specifies the CIDR block for the public (DMZ) subnet located in Availability Zone 1.
Public Subnet 2	10.0.2.0/24	Specifies the CIDR block for the public (DMZ) subnet located in Availability Zone 2.
Private Subnet 1	10.0.1.0/24	Specifies the CIDR block for the private subnet located in Availability Zone 1.
Private Subnet 2	10.0.3.0/24	Specifies the CIDR block for the private subnet located in Availability Zone 2.
Key name	Requires input	Specifies the public/private key pair that allows you to connect securely with your instance after it launches. When you create an AWS account, this is the key pair you created in your preferred region.
Transit tag	Transit	Specifies the tag is used by the Security Management Server to provision the Security Gateways automatically. Must contain up to 12 alphanumeric characters. Must be unique for each Quick Start deployment.
Allow upload and download	True	Specifies whether to download automatically the Software Blades contracts and other important data. Improves product experience by sending data to Check Point.

Configuration of Check Point CloudGuard IaaS Transit Gateways:

Parameter name	Default	Description
`Instance type`	`c4.xlarge`	Specifies the EC2 instance type for the Security Gateway.
`BGP ASN`	`65000`	Specifies the organization Autonomous System Number (ASN) that identified the routing domain for the Security Gateways.
`License`	`R80.10-BYOL`	Specifies the license to use for the Security Gateways. See Step 2 (on page 13) for the licensing options. You must have a subscription to the corresponding AMI in the AWS marketplace.
`Password hash`	Optional	Specifies the administrator password hash. Use this command to get the password hash: `openssl passwd -1 <PASSWORD>`
`SIC key`	Requires input	Specifies the one-time Activation Key. Enter a string that consists of at least 8 alphanumeric characters.

Configuration of the Check Point CloudGuard IaaS Security Management Server:

Parameter name	Default	Description
`Deploy management server`	`Yes`	Configure "`No`", if you want: • To use an existing Security Management Server, or to deploy a Security Management Server later. • To ignore the other parameters of this section.
`Default VPN access`	`Drop`	If the Spoke VPCs are trusted, you can configure "`Accept`" to allow all traffic between the Spoke VPCs.
`Instance type`	`m4.xlarge`	Specifies the EC2 instance type of the Security Management Server.
`License`	`R80.10-PAYG-MGMT5`	Specifies the license to install on the Security Management Server.
`Password hash`	Optional	Specifies the administrator password hash. Use this command to get the password hash: `openssl passwd -1 <PASSWORD>`
`Default Blades`	`On`	Configure "`Off`", if you want to disable the IPS, Application Control, Anti-Virus, and Anti-Bot Software Blades. After the deployment, you can manually enable and disable these and additional Software Blades.

Parameter name	Default	Description
`Administrator addresses`	Requires input	Specifies the allowed IP addresses, from which you can connect to the Security Management Server with HTTP, HTTPS, SSH, and GUI clients.
`Gateways addresses`	`10.0.0.0/16`	Specifies the CIDR IP range that is permitted to access the Security Management Server. Only gateways with IP addresses from this network can communicate with the Security Management Server.

Parameters for Deploying Security Transit into an Existing VPC

General Settings:

Parameter name	Default	Description
VPC	Requires input	Specifies the ID of your existing VPC.
Public Subnet 1	Requires input	Specifies the ID of an existing subnet inside the VPC for the first Security Gateway.
Public Subnet 2	Requires input	Specifies the ID of an existing subnet inside the VPC for the second Security Gateway.
Private Subnet 1	Requires input	Specifies the ID of an existing private subnet inside the VPC for the first Security Gateway.
Private Subnet 2	Requires input	Specifies the ID of an existing private subnet inside the VPC for the second Security Gateway.
Key name	Requires input	Specifies the public/private key pair that allows you to connect securely with your instance, after it launches. When you create an AWS account, this is the key pair you created in your preferred region.
Transit tag	Transit	Specifies that the Security Management Server uses this tag to provision the Security Gateways automatically. Must contain up to 12 alphanumeric characters. Must be unique for each Quick Start deployment.
Allow upload and download	True	Specifies whether to download automatically the Software Blades contracts and other important data. Improves product experience by sending data to Check Point.

Configuration of Check Point CloudGuard IaaS Transit Gateways:

Parameter name	Default	Description
`Instance type`	`c4.xlarge`	Specifies the EC2 instance type for the Security Gateway.
`BGP ASN`	`65000`	Specifies the organization Autonomous System Number (ASN) that identified the routing domain for the Security Gateways.
`License`	`R80.10-BYOL`	Specifies the license to use for the Security Management Server. See Step 2 (on page 13) for the licensing options. You must have a subscription to the corresponding AMI in the AWS marketplace.
`Password hash`	Optional	Specifies the administrator password hash. Use this command to get the password hash: `openssl passwd -1 <PASSWORD>`
`SIC key`	Requires input	Specifies the one-time Activation Key. Enter a string that consists of at least 8 alphanumeric characters.

Configuration of the Check Point CloudGuard IaaS Security Management Server:

Parameter name	Default	Description
`Deploy management server`	`Yes`	Configure "`No`", if you want: • To use an existing Security Management Server, or to deploy a Security Management Server later. • To ignore the other parameters of this section.
`Default VPN access`	`Drop`	If the Spoke VPCs are trusted, you can configure "`Accept`" to allow all traffic between the Spoke VPCs.
`Instance type`	`m4.xlarge`	Specifies the EC2 instance type of the Security Management Server.
`License`	`R80.10-PAYG-MGMT5`	Specifies the license to install on the Security Management Server.
`Password hash`	Optional	Specifies the administrator password hash. Use this command to get the password hash: `openssl passwd -1 <PASSWORD>`
`Default Blades`	`On`	Configure "`Off`", if you want to disable the IPS, Application Control, Anti-Virus, and Anti-Bot Software Blades. After the deployment, you can manually enable and disable these and additional Software Blades.

Parameter name	Default	Description
`Administrator addresses`	Requires input	Specifies the allowed IP addresses, from which you can connect to the Security Management Server with HTTP, HTTPS, SSH, and GUI clients.
`Gateways addresses`	`10.0.0.0/16`	Specifies the CIDR IP range that is permitted to access the Security Management Server. Only gateways with IP addresses from this network can communicate with the Security Management Server.

Configuring the Environment after the Deployment

You can use these values displayed in the **Outputs** tab to configure the environment later:

Key	Description
`SpokeTag`	Specifies the tag to put on the spoke VPC.
`ManagementName`	Specifies the name that represents the Security Management Server.
`CommunityName`	Specifies the name of the VPN Community created on the Security Management Server.
`ConfigurationTemplateName`	Specifies the name that represents the configuration template. Configurations required to provision the Gateways automatically in the Auto Scaling Group are placed in this template name. For example, what Security Policy to install, which Software Blades to enable, and so on.
`PublicAddressA`	Specifies the Public IP address of the first gateway.
`PublicAddressB`	Specifies the Public IP address of the second gateway.
`ManagementPublicAddress`	Specifies the public IP address of the Security Management Server.
`ControllerName`	Specifies the name that represents the controller. Configurations required to connect to your AWS environment are placed in this controller template name. For example, credentials and regions.

Step 4: Reviewing and Testing the Deployment

Review the deployment in the AWS Management Console and in Check Point SmartConsole.

If the set up was successful, you should see these components:

- Two Check Point CloudGuard Security Gateways in the Amazon EC2 Console.
- Two Gateways provisioned successfully in SmartConsole.
- Check Point IPsec VPN Software Blade is enabled, on each Security Gateway.
- Star VPN Community with both gateways, each configured as a Center Gateway.
- Security Policy with a Directional VPN rule exists.
- The Security Policy is installed successfully on the Security Gateways.

Check Point CloudFormation Templates

In This Section:

Template Parameters 23
Parameter Description.....23

Template Parameters

The section that follows, provides additional information about Check Point CloudFormation template parameters:

- Password hash
- SIC key
- IAM permissions (STS accounts)

Parameter Description

Parameter	Description

`Password hash`	To manage the environment security, administrators can connect to the Security Management Server with SmartConsole clients and to Check Point instances through the Gaia Portal.
	When you deploy a Check Point CloudGuard IaaS instance, you can set the administrator password for the server with 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.
	• On a Check Point Security Management Server, run this command:
	`cpopenssl passwd -1 password`
	• On Linux or Windows machines with OpenSSL installed, run this command:
	`openssl passwd -1 password`

`Secure Internal Communication (SIC) key`	The 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.
`IAM permissions`	When you set STS Role ARN values in the **STS Role** field of the Transit Management CloudFormation template, the role you create will have **sts:AssumeRole** permission. If you have to add or remove additional spoke accounts later, edit the Transit role profile in AWS, and add or remove ARNs.

Additional Features

In This Section:

Configuring VPN between the Transit CloudGuard Gateways and Your On-Premises Gateway 24
Tagging a Spoke VPC 24
Setting a Role on a Spoke VPC Account 25
Multi-Hub Support 26
Exporting Custom Routes to Spokes 27
Enabling Custom Routes to Spokes 27
Ignore Manually Created VPN Connections 29
Ignore Manually Created Customer Gateways 29
Changing the ASN of the Transit Gateway 29
Running Transit and Auto-Scaling Simultaneously 31
Deploying a Security Management Server Without an Internet Connection 32

Configuring VPN between the Transit CloudGuard Gateways and Your On-Premises Gateway

It is possible to connect your Corporate Gateway to the Transit hub. To do so, create a VPN tunnel on each CloudGuard Gateway towards the Corporate Gateway.

The customer manually performs the provisioning of VPN towards the Corporate Gateway.

- To create VPN and configure BGP on the on-premises gateway towards the Transit Gateways:

  Follow sk120534 http://supportcontent.checkpoint.com/solutions?id=sk120534 - Section "**(4-C) Creating the Transit VPC - Configure VPN Tunnel Interface on the on-premises Security Gateway**".

- To configure BGP on the Transit VPC gateways toward the on-premises gateways:

  Follow sk120534 http://supportcontent.checkpoint.com/solutions?id=sk120534 - Section "**(5-C) Connecting Transit VPC to Spoke VPCs - Configure Gaia OS on CloudGuard Gateways for AWS**".

For more information, see about the Transit VPC Architecture, see sk120534 http://supportcontent.checkpoint.com/solutions?id=sk120534.

Tagging a Spoke VPC

Step	Description
1	Create the spoke VPC and its subnets.
2	Edit the VPC and add this tag: Tag key: `x-chkp-vpn` Tag value: *<MANAGEMENT-NAME>/<VPN-COMMUNITY-NAME>* Where: • *<MANAGEMENT-NAME>* - Specifies the name of the Security Management Server. Use the same name you used when you executed the `autoprov_cfg` utility (on page 35). • *<VPN-COMMUNITY-NAME>* - Specifies the name of the VPN Community. Use the same name you used when you created the VPN Community (on page 38).

To connect a spoke VPC to multiple VPN communities, see *Multi-Hub Support* (on page 26).

To unlink a spoke, remove the tag. This deletes the transit configuration automatically.

Note - If an AWS Virtual Private Gateway (VGW) does not already exist, transit creates it and propagates routes from it, only to the main route table of the VPC. Make sure that all the subnets you want to use with transit, are associated with the main route table.

Setting a Role on a Spoke VPC Account

Important:

- This configuration is required only if you plan to deploy a spoke VPC in an AWS account, other than the AWS account, where the Transit VPC is deployed.
- You have to return to those steps for all other AWS accounts, into which you deploy a spoke.

Launch the **Cross Account Permissions** AWS CloudFormation template on the trustee (spoke) account.

Direct Link to AWS Cross Account Permissions Template
https://console.aws.amazon.com/cloudformation/home?#/stacks/create/review?templateURL=https%3A%2F%2Fs3.amazonaws.com%2FCloudFormationTemplate%2Fsts-role.yaml&stackName=Check-Point-STS .

For more information, see sk122074
http://supportcontent.checkpoint.com/solutions?id=sk122074.

Parameters for deploying the STS Role template:

Parameter label (name)	Default	Description
Trusted Account ID (Trusted account)	Requires input	A 12-digit number that represents the ID of the Transit VPC account. Enter that number.
IAM Role Permissions (Permissions)	Read-only	**Important** - You must select **Create with read-write permissions**.

- The template creates an AWS IAM role with all the permissions required for the Security Management Server to provision resources in the spoke VPC account.
- To review your newly created trust relationship, find the new role in the AWS IAM dashboard. Confirm the Transit VPC account number appears on the **Trust Relationship** tab.

Use the value that is displayed on the **Outputs** tab to configure the environment afterwards.

Key	Description
Role	AWS ARN for the new role you created. Use this role in the STS Role field in the deployment of the Check Point Security Management Server.

Note - You will be able to add or remove additional spoke accounts later. To do that, edit the Security Management Server Role profile in AWS and add or remove ARNs.

Multi-Hub Support

You can connect a spoke VPC to more than one Transit Hub.

For example, the first Transit Hub serves for Internet outbound traffic and the second Transit Hub serves for the corporate and spoke-to-spoke traffic.

To configure Multi-Hub support:

Step	Description
1	Connect to the command line on the Check Point Security Management Server.
2	Log in to the Expert mode.

3	Use the `config-community.sh` script (on page 38) to configure a separate Star VPN Community for each Transit Hub:
	`/etc/fw/scripts/autoprovision/config-community.sh "<VPN_COMMUNITY_NAME_1>"`
	`/etc/fw/scripts/autoprovision/config-community.sh "<VPN_COMMUNITY_NAME_2>"`

4	Use the `autoprov_cfg` CLI tool (on page 35) to add both Star VPN communities to the Controller: `autoprov-cfg set controller AWS -cn "<CONTROLLER_NAME>" -com "<VPN_COMMUNITY_NAME_1>,<VPN_COMMUNITY_NAME_2>"`

5	Use the `autoprov_cfg` CLI tool (on page 35) to create a new template for each Transit Hub:
	`autoprov_cfg add template -tn "<TEMPLATE_NAME_1>" -otp "<PASSWORD>" -ver R80.10 -po "<POLICY_NAME>" -vpn -vd "<VPN_DOMAIN_1>" -com "<VPN_COMMUNITY_NAME_1>"`
	`autoprov_cfg add template -tn "<TEMPLATE_NAME_2>" -otp "<PASSWORD>" -ver R80.10 -po "<POLICY_NAME>" -vpn -vd "<VPN_DOMAIN_2>" -com "<VPN_COMMUNITY_NAME_2>"`

6	On the AWS CloudFormation service, deploy the Transit template for both hubs.

Step	Description
7	For each spoke VPC, add a tag (on page 24). The tag will include information on all the Hubs, separated by a colon. • **Key:** `x-chkp-vpn` • **Value:** *<MANAGEMENT_NAME>/<VPN_COMMUNITY_NAME_1>*:*<MANAGEMENT_NAME>/<VPN_COMMUNITY_NAME_2>*

Important - If you add or remove a Transit Hub to an existing Hub, the configuration on all existing spokes is removed. This creates a Multi-Hub configuration for each spoke VPC. That causes reprovisioning of all the VPN connections and it may take time to finish. For example, when you design a Multi-Hub topology.

Expect downtime during the reconfiguration of the spoke VPCs. Schedule a maintenance window to perform these configuration steps. The amount of downtime it takes, depends on the number of tunnels you have.

Exporting Custom Routes to Spokes

By default, BGP settings export "all Internet (0.0.0.0/0)" CIDR to the spoke. This means that outgoing traffic from the spoke VPC is routed to the Transit Gateways.

There may be times that you want to export specific custom routes, instead of "all Internet". For example, in a Multi-Hub architecture where one hub handles the outbound traffic to the Internet, and the second Transit Hub serves for the spoke-to-spoke traffic. Another example is a single Transit hub environment, which enables spoke-to-spoke communication without allowing Internet access.

Enabling Custom Routes to Spokes

To configure a specific route, you have to configure two additional BGP routemaps:

Routemap	Description
spoke-routes	Name for a BGP routemap that contains all spoke CIDRs. This routemap is automatically created on the Transit Gateway and exported to the spokes, to enable all spoke-to-spoke traffic. **Important** - Do not use the name of a routemap that you have already defined on the Security Gateway, or a routemap that you want to manage manually. If you do so, this routemap will be overridden by the automation.
export-routes	Name for a BGP routemap that will also be exported to the spokes. The user has to create and manage this routemap on all Transit Gateways. This routemap can contain any routes you want to export to the spoke. For example, the route of a corporate network CIDR. **Important** - If you want to enable custom routes, you must enable the routes **before** you connect any spoke VPC to the Transit. If there are already spoke VPCs connected to the VPC and you want to enable custom routes, you have to disconnect them from the Transit: a) Remove the tag from the spoke VPC to disconnect it from Transit. b) Configure custom routes. c) Add the tag to reconnect the spoke.

To enable custom routes on the Security Management Server, run the `config-community.sh` script:

```
$FWDIR/scripts/autoprovision/config-community.sh "<VPN-COMMUNITY-NAME>"
[<SPOKE-ROUTES> [<EXPORT-ROUTES>, <EXPORT-ROUTES> ...]]
```

Replace these variables with the names in your configuration:

- "*<VPN-COMMUNITY-NAME>*"
- *<SPOKE-ROUTES>* (there can only be one *<SPOKE-ROUTE>* map)
- *<EXPORT-ROUTES>* (multiple *<EXPORT-ROUTE>* names can be added, separated by a comma)

IMPORTANT

- After you add a new VPN Community, you must also add each Security Gateway of the new hub as a Center Gateway in the VPN Community. The Transit service automatically identifies new Transit CloudFormation stack deployments. Therefore, you have to add Security Gateways to the correct VPN Community that you defined with the `autoprov_cfg` (on page 35) for this configuration template.
- The `config-community.sh` does not add Security Gateways as hub.
- We recommend that you stop the service when you add a new hub.

Ignore Manually Created VPN Connections

The Transit service scans all VPN connections in the region of a spoke VPC and tries to create interoperable device objects and VTI that match these connections.

If you want to create a VPN connection to a Transit Hub CloudGuard Security Gateway manually, add a tag to the AWS VPN connection object. This will cause the automation to ignore it.

Key: `x-chkp-vpn`

Value: `ignore`

Ignore Manually Created Customer Gateways

As part of the Transit automation work, the Transit service is also responsible to create the AWS customer gateway objects on each spoke VPC region/account.

The service deletes all customer gateways when they are not referenced by a VPN Connection. If you want to preserve your manually created customer gateways, add a tag on the AWS customer gateway object. This will cause the automation to ignore it.

Key: `x-chkp-vpn`

Value: `ignore`

Changing the ASN of the Transit Gateway

Important - Changing the Autonomous System number can be dangerous and can harm the internal data structures used by the Transit service. Make sure to edit only the AS number digits when you change the comment field.

A unique AS value is set for the Transit Gateways as part of the CloudFormation Template attributes. You cannot change the AS value through the AWS CloudFormation templates or through SmartConsole. You can change it through the AWS Console, or the Gaia Portal.

To change the ASN on the Transit Gateway:

Step	Description
1	In the AWS Console, remove the **x-chkp-vpn** tag from all spoke VPCs. Wait for all the AWS VPN and Check Point resources to be removed. Make sure no interoperable devices remain that are related to the resources you removed.
2	On the Security Management Server, stop the service: a) Connect to the command line the Security Management Server. b) Log in to the Expert mode. c) Stop the service: `service cme stop` This ensures that no new tags on the spoke VPCs are identified during this process.

3	Configure the Autonomous System number on the Transit Gateway in one of these ways:
	In Gaia Clish:
	a) Connect to the command line on the Transit Gateway.
	b) Log in to the Gaia Clish.
	c) Configure the AS:
	`set as <AS_Number>`
	d) Save the configuration:
	`save config`
	In Gaia Portal:
	a) Connect with a web browser to the Transit Gateway at:
	`https://<Gaia Management IP Address>`
	b) From the left tree, click **Advanced Routing > BGP**.
	c) In the **BGP Global Settings** section, click the **Change Global Settings** button.
	d) In the **Autonomous System** section, select **Local Autonomous System Number**.
	e) Enter the AS number.
	f) Click **Save**.

Step	Description
4	On the Security Gateway examine the new AS number: a) Connect to the command line the Security Gateway. b) Log in to the Expert mode. c) Run: `config-vpn show`
5	Connect with SmartConsole to Security Management Server.
6	The Transit service uses the **Comment** field to store configuration attributes. a) Find the @ sign. The old AS value follows it. b) Edit the value and replace the old value with the new AS value. Example: `{tags=managed-virtual-gateway|__once__|__load_balancer__|__template__MyTemplate|__vpn__192.168.1.1@65001}`
7	Repeat the steps above on all Security Gateways in the Transit Hub.
8	Add tags back to all related Spoke VPCs.
9	On the Security Management Server, start the service: `service cme start`
10	Wait for the new resources to provision. New Customer gateway objects are created. VPN Tunnels and BGP configurations are created with the new AS value on each gateway.

Running Transit and Auto-Scaling Simultaneously

To run Check Point Auto Scaling in AWS on the same Security Management Server that runs Transit:

Step	Description
1	Connect to the command line the Security Management Server.
2	Log in to the Expert mode.
3	Use the `autoprov_cfg` CLI tool (on page 35) to add the `-slb` attribute to the main Controller: `autoprov_cfg set controller AWS -cn "<CONTROLLER-NAME>" -slb`
4	Use the `autoprov_cfg` CLI tool (on page 35) to create an additional template for the auto-scale gateway: `autoprov_cfg add template -tn "<NEW-TEMPLATE-NAME>" -otp "<SIC-KEY>" -ver R80.10 -po "<POLICY-NAME>"`

For more information about configuring Auto Scaling in AWS, see sk112575 http://supportcontent.checkpoint.com/solutions?id=sk112575.

Deploying a Security Management Server Without an Internet Connection

It is mandatory that you have an Internet connection when you deploy the Security Management Server CloudFormation template. The CloudFormation template needs an Internet connection to confirm the deployment was successful.

If the Security Management Server instance cannot be reached over the Internet, the CloudFormation deployment will fail and the CloudFormation stack is reverted.

To deploy a Security Management Server without an Internet connection:

Step	Description
1	In the CloudFormation template: a) Go to **Check Point Settings > Installation Type**. b) Select **Manual Configuration**. c) Wait for the instance deployment to complete.
2	Connect with a web browser to the Security Management Server at: `https://`*<Gaia Management IP Address>*
3	Enter the username **admin**, and the password you entered on the CloudFormation template.
4	Click **Login**. The Gaia First Time Configuration Wizard opens.
5	Follow the instructions on the screen.

Advanced Configuration

In This Section:

Deploying and Configuring the Check Point Security Management Server.....33
Configuring the Multi-Domain Server.....39

Deploying and Configuring the Check Point Security Management Server

Required Permissions for the Security Management Server

The Security Management Server must have these IAM permissions:

- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeSubnets`
- `ec2:DescribeInstances`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeTags`
- `elasticloadbalancing:DescribeListeners`
- `elasticloadbalancing:DescribeTargetGroups`
- `elasticloadbalancing:DescribeRules`
- `elasticloadbalancing:DescribeTargetHealth`
- `autoscaling:DescribeAutoScalingGroups`
- `ec2:DescribeCustomerGateways`
- `ec2:CreateCustomerGateway`
- `ec2:DeleteCustomerGateway`
- `ec2:DescribeRouteTables`
- `ec2:EnableVgwRoutePropagation`
- `ec2:DisableVgwRoutePropagation`
- `ec2:DescribeVpnGateways`
- `ec2:CreateVpnGateway`
- `ec2:AttachVpnGateway`
- `ec2:DetachVpnGateway`
- `ec2:DeleteVpnGateway`
- `ec2:DescribeVpnConnections`
- `ec2:CreateVpnConnection`

- `ec2:DeleteVpnConnection`
- `cloudformation:DescribeStacks`
- `cloudformation:DescribeStackResources`
- `cloudformation:CreateStack (resource: arn:aws:cloudformation:*:*:stack/vpn-by-tag--*/*)`
- `cloudformation:DeleteStack (resource: arn:aws:cloudformation:*:*:stack/vpn-by-tag--*/*)`

Deploying the Security Management Server

If you have a Check Point Security Management Server on AWS already (version 317 or higher), or on-premises Check Point Security Management Server R80.10 with R80.10 Jumbo Hotfix Take 135 (or higher), you can use it to manage the Transit VPC Security Gateways.

Location of the Management Server	Instructions
Security Management Server in AWS	To deploy a new Security Management Server in AWS, see sk130372 http://supportcontent.checkpoint.com/solutions?id=sk130372 > Section **Installing the Check Point Security Management Server**. **Note -** Make sure to select **Create with read-write** permissions in the **IAM role** dropdown field. This is required to include these permissions in the IAM policy of the IAM role attached to the Security Management Server.
Security Management Server on-premises	To deploy a new Security Management Server on-premises, or use an existing Security Management Server on-premises, see sk130372 http://supportcontent.checkpoint.com/solutions?id=sk130372 > Section **Deploying a Security Management Server on-premises**.

Configuring the Security Management Server

In This Section:

Configuring the Security Management Server with the 'autoprov-cfg' Tool.....35
Configuring the VPN Community with the 'config-community.sh' Script 38
Configuring the Access Control Policy 38

Follow the instructions below to configure the Transit service, which controls CloudGuard's integration to AWS Endpoints that seamlessly operate the AWS Transit Hub solution.

Examples of other configuration are in the *Examples of autoprov-cfg Configurations* (on page 36) section.

Configuring the Security Management Server with the 'autoprov-cfg' Tool

This tool configures the Check Point Security Management Server with all the settings needed for Transit:

Step	Description
1	Connect to the command line on the Check Point Security Management Server.
2	Log in to the Expert mode.
3	Run all the commands below. Commands and their description: • `autoprov_cfg init AWS -mn "<MANAGEMENT-NAME>" -tn "<TEMPLATE-NAME>" -otp "<SIC-KEY>" -ver R80.10 -po "<POLICY-NAME>" -cn "<CONTROLLER-NAME>" -r "<REGIONS>" -iam` Initializes configuration with IAM credentials. Options: • `-mn` - Specifies the name of the Security Management Server • `-tn` - Specifies the template name • `-otp` - Specifies the one-time SIC password • `-ver` - Specifies the Gateway version • `-po` - Specifies the name of the policy package • `-cn` - Specifies the name of the Controller • `-r` - Specifies the list of regions, separated by commas • `-iam` - Specifies to use IAM to connect to AWS

Step	Description
	• `autoprov_cfg set controller AWS -cn "<CONTROLLER-NAME>" -sg -sv -com "<VPN-COMMUNITY-NAMES>" -sn "<SUBACCOUNT-NAME>" -ssr "<STS-ROLE-ARN>"` Sets Controller with the required attributes for transit. Options: • `-sg` - Specifies to scans gateways (enables Autoprovision) • `-sv` - Specifies to scan VPN (enables Transit) • `-com` - Specifies the list of VPN communities allowed to be used by this Controller • `-sn` - Specifies the custom name for your sub-account • `-ssr` - Specifies the STS role name of trustee (spoke account) • `autoprov_cfg set template -tn "<TEMPLATE-NAME>" -vpn -vd "<VPN-DOMAIN>" -com "<VPN-COMMUNITY-NAME>"` Sets template with the required attributes for transit. Options: • `-vpn` - Enables the IPsec VPN blade on gateways • `-vd` - Specifies the name of the VPN Domain object • `-com` - Specifies the name of the VPN Community • `autoprov_cfg show all` Shows all the used configurations. Run this command to confirm all the configurations are correct.
4	Run this command to test the configuration: `service cme test` Make sure there are no errors. If the test ends with any error, see the *Troubleshooting* section.

Examples of 'autoprov_cfg' Configuration

Learn how to use the `autoprov_cfg` CLI tool (on page 35) to configure different deployment scenarios.

In the examples below, replace the **bolded** variables, with values in your environment.

Example 1 - Management, Transit, and spoke VPCs are all on the same account

Scanning the Transit and spoke account is authenticated using the management IAM role only.

Step	Syntax
1	`autoprov_cfg init AWS -mn "my-mgmt" -tn "my-template" -otp "my-one-time-password" -ver R80.10 -po "my-policy" -cn "my-controller" -r "us-east-1" -iam`
2	`autoprov_cfg set controller AWS -cn "my-controller" -sg -sv -com "my-vpn-community"`
3	`autoprov_cfg set template -tn "my-template" -vpn -vd "my-vpm-domain" -com "my-vpn-community"`

Example 2 - Management and Transit are on the same account, but the spoke VPC is on a different account

Add a sub-account to the Controller with an STS role on the spoke account for spoke scanning.

The Management IAM role scans the transit account.

Step	Syntax
1	`autoprov_cfg init AWS -mn "my-mgmt" -tn "my-template" -otp "my-one-time-password" -ver R80.10 -po "my-policy" -cn "my-controller" -r "us-east-1" -iam`
2	`autoprov_cfg set controller AWS -cn "my-controller" -sg -sv -com "my-vpn-community" -sn "my-account" -ssr "arn:aws:iam::123456789012:role/SpokeAccountRole"`
3	`autoprov_cfg set template -tn "my-template" -vpn -vd "my-vpm-domain" -com "my-vpn-community"`

Example 3 - Management, Transit, and spoke VPC are each on their own account, and trust is done with STS roles

Trust between the management and transit accounts is done with STS roles.

Add a sub-account to the Controller with an STS role on the spoke account to allow spoke scanning.

Add an STS role for the transit account on the Controller to scan gateways.

Step	Syntax
1	`autoprov_cfg init AWS -mn "my-mgmt" -tn "my-template" -otp "my-one-time-password" -ver R80.10 -po "my-policy" -cn "my-controller" -r "us-east-1" -iam`
2	`autoprov_cfg set controller AWS -cn "my-controller" -sg -sv -com "my-vpn-community" -ssr "arn:aws:iam::210987654321:role/TransitAccountRole" -sn "my-account" -ssr "arn:aws:iam::123456789012:role/SpokeNameOne"`
3	`autoprov_cfg set template -tn "my-template"`

Example 4 - Management, Transit, and spoke VPCs are each on their own account, and a user with programmatic access is set on the transit account

Management, Transit, and spoke VPCs are each on their own account. A user with programmatic access is set on the transit account.

Add a sub-account to the Controller with an STS role on the spoke account for spoke scanning.

Add an access key and a secret key of a user with programmatic access on the transit account on the Controller, to scan gateways.

Step	Syntax
1	`autoprov_cfg init AWS -mn` **"my-mgmt"** `-tn` **"my-template"** `-otp` **"my-one-time-password"** `-ver` **R80.10** `-po` **"my-policy"** `-cn` **"my-controller"** `-r` **"us-east-1"** `-ak` **AKIKBJKKGPVSLTTVCGFU** `-sk` **m97031r93aa7x6plnkdum97031r93aa7x6plnkdu**
2	`autoprov_cfg set controller AWS -cn` **"my-controller"** `-sg -sv -com` **"my-vpn-community"** `-sn` **"my-account"** `-ssr` **"arn:aws:iam::123456789012:role/SpokeNameOne"**
3	`autoprov_cfg set template -tn` **"my-template"** `-vpn -vd` **"my-vpm-domain"** `-com` **"my-vpn-community"**

Configuring the VPN Community with the 'config-community.sh' Script

This script creates a VPN Community with all the settings needed for Transit:

Step	Description
1	Connect to the command line on the Check Point Security Management Server.
2	Log in to the Expert mode.

3	Run:
	`/opt/CPcme/menu/additions/config-community.sh "<`*VPN-COMMUNITY-NAME*`>"`
	Example:
	`/opt/CPcme/menu/additions/config-community.sh "Transit-VPN-Community"`

Configuring the Access Control Policy

Step	Description
1	Connect with SmartConsole to your Check Point Security Management Server.
2	If the Security Management Server and the Security Gateway have to communicate through public IP addresses, make sure that the Security Management Server object is defined with the elastic IP address. Edit the Security Management Server object and change the IP address. **Important -** If you change the main IP address of the Security Management Server, you must issue and install the license(s) for the new IP address.

Step	Description
3	Create the Security Policy you want to install on the Transit Gateways. When you name the policy package, use the package name you set when you executed the `autoprov_cfg` (on page 34) utility.
4	We recommend you create an explicit VPN Directional rule in the Access Control Policy to allow the required services to work over the VPN tunnels:
4A	Enable the support for VPN directional rules: 1. In SmartConsole, click **Menu > Global properties**. 2. In the left tree, click **VPN > Advanced**. 3. Select **Enable VPN Directional Match in VPN Column**. 4. Click **OK**.

4B	Create an explicit VPN Directional rule:
	• **Source** - Applicable Objects
	• **Destination** - Applicable Objects
	• **VPN** - All these:
	  • `Community -> Community`
	  • `Community -> Internal_clear`
	  • `Internal_clear -> Community`
	• **Services & Applications** - Applicable Services
	• **Action** - `Accept`
	• **Track** - `None`, or `Log`
	• **Install On** - Transit gateways

5	Install the Access Control Policy on the Transit gateways.

Configuring the Multi-Domain Server

Step	Description
1	Connect to the command line on the Check Point Multi-Domain Server.
2	Log in to the Expert mode.
3	Execute the `autoprov_cfg` tool on the Multi-Domain Server. See sk120992 http://supportcontent.checkpoint.com/solutions?id=sk120992.
4	Execute the `config-community.sh` script on the Multi-Domain Server: `env MGMT_CLI_DOMAIN="<DOMAIN_NAME>" /etc/fw/scripts/autoprovision/config-community.sh "<VPN-COMMUNITY-NAME>" [<SPOKE-ROUTES> [<EXPORT-ROUTES>, <EXPORT-ROUTES> ...]]` Replace the "<*DOMAIN_NAME*>" with the name of your Domain.
5	Tag a spoke VPC on a Multi-Domain Server. On a Multi-Domain Server, you have to indicate the specific Domain, on which Transit has to manage the VPN connection to the spoke VPC. Therefore, the tag value structure for the spoke VPC also must have the Domain name. Tag key: `x-chkp-vpn` Tag value: <*MANAGEMENT_NAME*>/<*DOMAIN_NAME*>/<*VPN_COMMUNITY_NAME*> Where: • <*MANAGEMENT_NAME*> - Specifies the name of your Multi-Domain Server. Use the same name you used when you executed the `autoprov_cfg` command. • <*DOMAIN_NAME*> - Specifies the name of the Domain as defined in the SmartConsole. • <*VPN_COMMUNITY_NAME*> - Specifies the name of your VPN Community. Use the same name you used when you created the VPN Community (on page 38).

Troubleshooting

Issue	Solution
Where are the service logs?	Examine this log file: • On Security Management Server: `$FWDIR/log/autoprovision.elg` • On Multi-Domain Server: `$MDS_FWDIR/log/autoprovision.elg` You do not need to enable any additional debugging to view the full log.
Management Server does not recognize the `autoprov_cfg` command.	The latest add-on package is not installed on your Management Server. Download and install the latest version. See sk130372 http://supportcontent.checkpoint.com/solutions?id=sk130372.
The `service cne test` command fails with this error: `Exception: 'Your management version does not support "get-interfaces"'`	Your Security Management Server is not supported. The Transit service can only run on a Check Point Security Management Server on AWS versions 317 or higher. Install a supported version.
The `service cme test` command fails with this error: `Exception: Unauthorized Operation: You are not authorized to perform this operation.`	The Security Management Server IAM role is not set with read/write permissions, or trust between a spoke account and a management account is not configured properly. See the issue below "*What permissions are required for the Security Management Server IAM role?*" for an example of IAM role permissions required for the Security Management Server.

Issue	Solution

Transit Gateway is not provisioned, (does not show in SmartConsole).	• In the AWS Console, check that the Transit Gateway has these tags:
	Key Tag:
	`x-chkp-tags+`
	Key Value:
	`management=<name>+template=<name>+ip-address=<public|private>`
	Check that the value of the tag is configured properly. If not, change or add it accordingly.
	• Confirm that the names of the management and template are the same that you configured with the `autoprov_cfg` utility.
	• Confirm the IP address is set correctly to the value, "`public`" OR "`private`".
	• Confirm that the management instance can reach the public or private IP address of the Transit Gateway. If not, configure the applicable route.

Connection to the Transit Gateway is lost after the restrictive policy is installed for the first time, and the policy cannot be installed again on the Transit Gateway.	The Transit Gateway is configured to connect to the Security Management Server with the public IP address (the elastic IP address), but the Security Management Server in SmartConsole is configured with the private IP address. 1. Edit the Security Management Server object in SmartConsole and change the IP address to the public IP address. Note - This change requires to issue the licenses for the new IP address. 2. Delete the gateway instance. It cannot be recovered at this point. 3. Deploy Transit Gateways with the CloudFormation template again.
The `autoprovision.elg` file shows this error: `Exception: There is already a VPN connection with different option value.`	These are manually created VPN connections in the region of the spoke VPC. See *Ignore Manually Created VPN Connections* (on page 29).
The `autoprovision.elg` file shows this error: `Exception: Ambiguous gateway by address <IP address> for <Name of Interoperable Object>`	The Transit Gateway is set as the Center Gateway in more than one VPN Community defined for the Controller. Remove the Transit Gateway from all other VPN communities.

Issue	Solution

There is no spoke-to-spoke communication for some traffic, although ICMP pings between the spokes can pass.	• Confirm the Security Policy is not blocking the traffic.
	• On the gateway, run:
	`cat $PPKDIR/boot/modules/simkern.conf`
	Confirm the file exists and contains this line:
	`sim_ipsec_dont_fragment=0`
	• If there is still no traffic between spokes, lower the MTU on the interfaces of hosts deployed in the spoke VPCs to be lower than 1500.

Issue	Solution
What permissions are required for the Security Management Server IAM role?	The JSON script below is an example of a spoke account role ARN. Change the values in the parameters to reflect those in your environment: `arn:aws:iam::<`*123456789012*`>:role/<`*RoleNameOne*`>` Example of a JSON script:

```
{
    "Version": "2012-10-17",
    "Statement":
     [
         {
         "Action": [
                   "sts:AssumeRole"
                   ],
         "Resource": [
                     "arn:aws:iam::123456789012:role/RoleNameOne",
                     ],
         "Effect": "Allow"
         },
         {
         "Action": [
                   "ec2:DescribeInstances",
                   "ec2:DescribeNetworkInterfaces",
                   "ec2:DescribeSubnets",
                   "ec2:DescribeVpcs",
                   "ec2:DescribeVpnGateways",
                   "ec2:DescribeVpnConnections",
                   "ec2:DescribeSecurityGroups",
                   "elasticloadbalancing:DescribeLoadBalancers",
                   "elasticloadbalancing:DescribeTags",
                   "elasticloadbalancing:DescribeListeners",
                   "elasticloadbalancing:DescribeTargetGroups",
                   "elasticloadbalancing:DescribeRules",
                   "elasticloadbalancing:DescribeTargetHealth",
                   "autoscaling:DescribeAutoScalingGroups"
                   ],
        "Resource": "*",
        "Effect": "Allow"
        },
        {
        "Action": [
                  "ec2:DescribeCustomerGateways",
                  "ec2:CreateCustomerGateway",
                  "ec2:DeleteCustomerGateway",
                  "ec2:DescribeRouteTables",
                  "ec2:EnableVgwRoutePropagation",
                  "ec2:DisableVgwRoutePropagation",
                  "ec2:DescribeVpnGateways",
                  "ec2:CreateVpnGateway",
                  "ec2:AttachVpnGateway",
                  "ec2:DetachVpnGateway",
                  "ec2:DeleteVpnGateway",
                  "ec2:DescribeVpnConnections",
                  "ec2:CreateVpnConnection",
                  "ec2:DeleteVpnConnection"
                  ],
         "Resource": "*",
         "Effect": "Allow"
         },
         {
         "Action": [
                   "cloudformation:DescribeStacks",
                   "cloudformation:DescribeStackResources"
                   ],
         "Resource": "*",
         "Effect": "Allow"
         },
         {
         "Action": [
                   "cloudformation:CreateStack",
                   "cloudformation:DeleteStack"
                   ],
          "Resource": "arn:aws:cloudformation:*:*:stack/vpn-by-tag--*/*",
          "Effect": "Allow"
          }
    ]
}
```

Issue	Solution
How do I add a Corporate Gateway, as an Externally Managed VPN Gateway to allow a secured VPN connection between the on-premises and the Transit Hub?	See sk120534 http://supportcontent.checkpoint.com/solutions?id=sk120534.
How do I configure Remote Access VPN through a Corporate Gateway to a Spoke VPC?	See sk120534 http://supportcontent.checkpoint.com/solutions?id=sk120534.
Transit Gateways are not added to the Management Server.	Check tags in the Transit Gateway and Transit Gateway Route Tables as described in the section *Deploying Security Transit Gateway Auto Scaling Group.*
I used the Transit Gateway First Time Configuration Wizard. However, the configuration is not correct.	You have these options: • Initialize all configuration by running the tool again. • Update only specific configuration with the `autoprov_cfg` tool. See the section *Deploying and Configuring the Check Point Security Management Server* (on page 33).
The `autoprov_cfg` command for configuring the template on the Management Server fails.	Before you define a VPN community for the template, it must be defined on the AWS Controller.

Limitations

- Check Point on-premises R80.10 Security Management Server is supported only when R80.10 Jumbo Hotfix Accumulator Take 142 (or above) is installed. See sk116380 http://supportcontent.checkpoint.com/solutions?id=sk116380.

  Note - Installation of the Check Point R80.10 Jumbo Hotfix Accumulator on the Security Management Server is supported only for Take 142 and above.

- Load Sharing Mode for Transit Gateway is not supported. Only High Availability Active/Standby deployment is available.

- To create a secured VPN connection between the on-premises and Transit Hub, you must manually configure the VPN connection, and route from Transit to the corporate network.

  See sk120534 http://supportcontent.checkpoint.com/solutions?id=sk120534 > Section **Creating the Transit VPC** > **Configure VPN Tunnel Interface on the on-premises Security Gateway**.

Additional Resources

- Amazon EC2 http://aws.amazon.com/ec2/
- Amazon VPC http://aws.amazon.com/vpc/
- AWS CloudFormation https://aws.amazon.com/CloudFormationTemplate/management.json
- AWS Auto Scaling https://aws.amazon.com/ec2/autoscaling/
- Check Point AWS CloudFormation: sk111013
  http://supportcontent.checkpoint.com/solutions?id=sk111013
- Check Point CloudGuard IaaS Auto Scaling documentation: sk112575
  http://supportcontent.checkpoint.com/solutions?id=sk112575
- Configuration of AWS STS to delegate access across two AWS accounts: sk122074
  http://supportcontent.checkpoint.com/solutions?id=sk122074
- Check Point CloudGuard for AWS - Transit VPC Architecture: sk120534
  http://supportcontent.checkpoint.com/solutions?id=sk120534