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.

Check Point CloudGuard Network for Nutanix R81 Deployment Guide

Latest Version of this Document in English
Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>27 June 2021</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
# Table of Contents

**Introduction** ................................................................................................................................ 5  
Costs and Licenses................................................................................................................................ 5  
Prerequisites........................................................................................................................................ 5  
Architecture ......................................................................................................................................... 6  
Solution Overview ................................................................................................................................. 6  
Use Cases............................................................................................................................................ 7  
Security Policy..................................................................................................................................... 8  

**Deployment Steps** ............................................................................................................................ 9  
Step 1: Install the CME Bundle on the Management Server ............................................................. 9  
Step 2: Configure the Management Server ......................................................................................... 9  
  
  Automatic Provisioning of CloudGuard Objects ............................................................................. 10  
Step 3: Upload CloudGuard Network Security Gateway Image to Prism Central ......................... 10  
Step 4: Create a Project in Nutanix Prism Central ............................................................................ 11  
Step 5: Import and Configure Nutanix Calm .................................................................................... 11  
Step 6: Apply Micro-Segmentation Policy Assignment ................................................................. 14  
  
  Service Chain Insertion ..................................................................................................................... 14  
  
  Configure Nutanix Flow to Route Traffic through the Service Chain ......................................... 14  
  
  (Optional) Deploy additional CloudGuard Network Security Gateways with Nutanix Calm Scale Out 15  
  
  Enabling the CloudGuard Controller .............................................................................................. 15  

**Troubleshooting and Best Practices** ................................................................................................. 17  

**Additional Resources** ..................................................................................................................... 18
Introduction

Check Point CloudGuard for Nutanix delivers multi-layered defense to protect East-West traffic in the Nutanix deployed data center. CloudGuard transparently enforces security at the hypervisor level and between Virtual Machines (VMs), and provides comprehensive visibility into Virtual Network traffic trends and threats. CloudGuard Network Security Gateway for Nutanix is automatically deployed as a service Virtual Machine (VM) in a virtual environment. The CloudGuard Gateway secures Nutanix Data Center traffic between VMs across the Virtual Network.

Check Point CloudGuard for Nutanix Flow meets organizational cloud security needs:

- Next-Generation Firewall with Application Control, Data Awareness, HTTPS Inspection, NAT, and logging
- IPS and virtual patching of cloud resource
- URL Filtering for Internet-bound traffic
- Anti-Bot and Anti-Virus, and Zero-day Threat Emulation and Threat Extraction
- Automated solution with Nutanix Calm

Costs and Licenses

Customers are responsible for the cost of the Nutanix services used, when they deploy the solution as described in this guide.

The Nutanix Calm Blueprint for the CloudGuard Network Security Gateway includes parameters that you can configure. Some of these features, such as Nutanix Flow, affect the cost and requirements for the deployment. For estimated costs, see Nutanix Software Editions & Licensing.

For CloudGuard Network Security Gateway Private Cloud Images, see sk158292.

The Check Point CloudGuard Security Gateways, Check Point CloudGuard Security Management Server, Nutanix Prism Central, Nutanix Calm Blueprint, and Nutanix Flow described in this guide must have a license.

The license for Check Point CloudGuard Security Gateways is Bring Your Own License (BYOL).

To buy BYOL licenses, contact Check Point Sales.

Prerequisites

Before you use this solution, make sure to read the Nutanix terms and services:

- Nutanix Prism Central
- Nutanix Calm
- Nutanix Flow

If you are new to Nutanix, see Getting Started with Nutanix.
Architecture

The diagram shows Check Point CloudGuard Network Security Gateway Solution for Nutanix Flow, a solution which includes:

- Nutanix Calm multi-cloud application management framework
- Nutanix Flow security feature that allows for firewall-type protection at the VM layer
- Nutanix AHV (Acropolis Hypervisor) enterprise-ready hypervisor
- Check Point Cloud Management Extension (CME), provides automatic provisioning of CloudGuard Network Security Gateways
- Prism Central, a centralized management solution for Nutanix environments
- Check Point R81 Security Management
- Check Point R81 CloudGuard Network Security Gateway

When integrated with Check Point CloudGuard Network Security Gateways, Nutanix Flow ability to control traffic is increased with the best threat prevention capabilities. Micro-segmentation can deduce the total sum of vulnerabilities, while it helps to secure your assets and data in the Nutanix Data Center against the most sophisticated threats with multi-layered protections including: Firewall, IPS, Application Control, Antivirus, Anti-Bot, and award-winning SandBlast Threat Emulation and Threat Extraction technologies.

Integration Diagram:

Solution Overview

When integrating with Check Point Network Security Gateways, Nutanix Flow’s ability to control traffic is augmented with industry leading threat prevention capabilities. Nutanix and Check Point have partnered to deliver an integrated solution with Check Point CloudGuard, which allows companies to realize the full potential of the SDDC and protect against potential vulnerabilities, malware, and other sophisticated threats. The joint solution for Nutanix Data Center effectively addresses one of the key challenges of modern data center networks, securing workloads at the perimeter with Check Point’s industry leading edge firewall.
CloudGuard Network Security Gateways are placed on each AHV host and controlled by Check Point Security Management.

**OVS Bridge Chain**

The bridge mode operation intercepts traffic and has the ability to block traffic before it is sent along. Bridge network functions have ingress and Egress interfaces. In the diagram, the HR VM traffic is redirected through a bridge CloudGuard Security Gateway. This configuration is deployed on each AHV host in the cluster.

**Use Cases**

These are examples of how you can set up your Nutanix Flow Gateway architecture.

**Micro-Segmentation**

Micro-Segmentation is a component of Nutanix Flow networking that simplifies policy management. Micro-Segmentation uses Multiple Prism Central categories (logical groups), a powerful, distributed firewall that gives administrators an application-centric policy management tool for securing traffic.
Micro-Segmentation helps deduce the sum of vulnerabilities, by preventing activities along the east-west traffic in the perimeter. This is established by deploying CloudGuard Network Security Gateways integrated with Nutanix Flow. Nutanix Calm Blueprint creates a service chain and Security Gateways on each AHV host. Together with Nutanix Flow, you can redirect traffic to the CloudGuard Network Security Gateway in the service chain for inspection, based on the user-defined Nutanix Flow Policy.

**Virtual Desktop Infrastructure**

Nutanix Flow can separate groups of virtual desktops with a Security Policy and work with CloudGuard Network Security Gateways on Acropolis Hypervisor (AHV) to examine and enforce application layer traffic and block threats across the virtual desktop infrastructure.

**Security Policy**

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

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

- Access Control
- Desktop Security
- Threat Prevention

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

When you configure the Check Point Security Management Server with the Cloud Management Extension (CME) utility, specify the name of the Security Policy package to install on the CloudGuard Network Gateways with the `-po` parameter. For the default Security Policy, use the value "Standard" (a capital "S" is required), for this parameter.

To configure more policy packages and install a different policy package on the Security Gateways deployed for the Nutanix Flow solution, then specify the policy package's name when you run `cme_menu`. Afterwards, create and configure the policy by connecting to your Security Management Server with SmartConsole.

For more information, go to the [CME R80.10 and above Administration Guide](#) and navigate to "CME Structures and Configurations".
Deployment Steps

Use the steps to deploy your Check Point CloudGuard Network Security Gateway for Nutanix Flow.

**Step 1: Install the CME Bundle on the Management Server**

The Cloud Management Extension (CME) is a utility that is installed and runs on Check Point Security Management Servers and Multi-Domain Security Management Servers in cloud platforms or on-premises.

**Important** - Keep CME up-to-date with Automatic Updates. To get CME with Automatic Updates, remove any CME installation made through CPUSE and refer to Check Point Upgrade Service Engine (CPUSE) - Gaia Deployment Agent for detailed installation instructions

**To install the CME utility:**

1. Go to [CME (Cloud Management Extension) for CloudGuard Latest Updates](#)
2. Download the latest CME package for your Management Server version.
3. Follow the Installation Instructions to install CME. See the [CME R80.10 and Above Administration Guide](#).

**Step 2: Configure the Management Server**

Configuring the CloudGuard Management Server Properties

Log in with SSH to the Management Server in Expert mode and run this command:

```
cme_menu
```

Configure the CloudGuard Management Server Properties. The controller is the Nutanix Prism Central. Before you can create new service, it is necessary to add the controller, Nutanix Prism Central, to your environment.

**To register a new controller:**

1. Navigate to the cme_menu.
2. Select Nutanix > Manage Nutanix Controllers > Add Nutanix Controller.
3. Enter the Nutanix Prism IP, which is the Nutanix Prism Central IP. When the thumbprint of the server shows, verify it. You can obtain the thumbprint from the Nutanix Prism Central CLI (ncli), log in as admin, and then run:

   ```
   openssl s_client -showcerts -connect <Prism Central IP>:9440 < /dev/null | openssl x509 -outform DER | sha256sum | cut -d" " -f1
   ```

4. Enter the **Controller Name**. This name must be unique for each controller on the Management Server.
5. Enter the **Controller User Name** (this is the same user name used to log in to the Prism Central). The user name must contain only English chars, numbers, and "_".
6. Enter the Controller User Password and then confirm (this is the same password used to log in into the Prism Central).
7. If this is a Multi-Domain Server environment, select the domain.
8. To confirm the controller is connected, select Show Nutanix Controller and make sure your Nutanix controller status is connected.

To add a Gateway template:

1. Navigate to the cme_menu.
2. Select Nutanix > Configure Gateway Parameters > Add Gateway Template.
3. Enter the SIC Key that is used to communicate with the Gateways.

   Note - The SIC Key must be the same for the Nutanix Calm Blueprint and the CME template for the autoprovision to succeed.

4. Enter the CloudGuard Network Security Gateway version that you plan to deploy.
5. To verify the template was created, select Nutanix > Configure Gateway Parameters > Show Existing Templates.

Automatic Provisioning of CloudGuard Objects

Automatic Provisioning handles these actions on CloudGuard objects:

- Creates CloudGuard objects on the CloudGuard Management Server when the gateway is ready.
- Automatically initializes SIC between the CloudGuard Gateway and the CloudGuard Management Server.
- Configures Identity Awareness on the CloudGuard Gateway.
- Installs Standard policy on new Security Gateways. Note - After the policy installation is complete, then you can use SmartConsole to install a different policy on the gateway.

To enable Automatic Provisioning:

After you create a new controller the Autoprovission service starts automatically.

To see the service status, run:

```
service cme status
```

To disable Automatic Provisioning:

If you want to stop the Autoprovission service, run:

```
service cme stop
```

⚠️ Important - The instructions for these Nutanix configuration were written for version PC.2020.11.0.1

Step 3: Upload CloudGuard Network Security Gateway Image to Prism Central

To start the deployment process, upload the Check Point CloudGuard Network Security Gateway for Nutanix AHV image to Prism central.
Important - These instructions are for version PC.2020.11.0.1

To upload the image to Prism Central:

1. Log into the Prism Central web UI.
2. Download CloudGuard Network Security Gateway R81 for Nutanix AHV. See sk158292 "CloudGuard for Private Cloud Images".
3. From the Prism Central menu, navigate to Virtual Infrastructure > from the entities menu select Images.
4. Select Add Image.
5. Browse to add a local image file > click OK.
6. In the Image Name field, enter a name (or accept the default value), a description (optional). Keep the Image Type set to Disk.
7. Click Save.

For more options, see Images Summary View.

Step 4: Create a Project in Nutanix Prism Central

A project defines a set of Active Directory with the common set of requirements or a common function, such as a team that collaborates on an engineering project.

To create a Project:

1. From the Prism Central menu, navigate to Services > Calm.
2. From the side toolbar, click Projects > Create Project.
3. Enter a Project Name and Description.
4. Click Select Provider > Nutanix.
5. Click Select Account and select the applicable account. To associate the interfaces on each CloudGuard Network Security Gateway instance in this project, select Clusters and Subnets.
6. (Optional) to specify use limits for compute, storage, and memory in the displayed vCPUs, Storage, and Memory fields, select Quotas.

For more options, see Project Configuration.

Step 5: Import and Configure Nutanix Calm

Calm is a multi-cloud application management framework delivered by Nutanix. Calm provides application automation and lifecycle management natively integrated into the Nutanix Platform. With Calm, applications are defined with simple blueprints that are easily created with the use of industry standard skills and control all aspects of the application’s lifecycle, such as provisioning, scaling, and cleanup.

To upload Blueprints:

1. From the Prism Central primary menu, navigate to Services > Calm.
2. Select Blueprints > click Upload Blueprint.
3. Browse the Check Point Gateway Calm Blueprint JSON file, select the project created in the previous section > click Upload.

Important - In the steps that follow, it is necessary to only change the settings in the value fields. Do not change the parameters or cloud-init script.
4. From the top toolbar, click **Credentials**. Add the **Credential Name**, **Username**, **Secret Type**, and **Password**. Enter the default Check Point admin password. **Note** – It is necessary to have a minimum of one credential in a blueprint. Click **Save**.

5. Fix the errors in the top (in the red exclamation mark box) and configure the settings in the Blueprint:
   a. Select the management NIC interface
   b. Select the CloudGuard Network Security Gateway Image uploaded to Prism Central in Step 3. **Do not** clear the checkbox next to **bootable**, the VM does not boot if the checkbox is not selected.

6. Click **Launch**.

**Parameters for the Calm instances**

7. In **Profile Configuration**, enter these parameters:
   - Enter the **Name** of the Nutanix Calm **Application**
   - Select the **Admin Shell**. The default value is `/etc/cli.sh`
   - Select if to **allow upload and download** Software Blade contracts and improve product experience by sending data to Check Point. The default value is **true**.
   - Enter the Admin user’s **password hash** in apostrophe ‘<password_hash>’. Use this command “openssl passwd –1 PASSWORD”
   - Enter the Check Point Gateway **SIC** key.

   **Note** - The SIC Key must be same for the Nutanix Calm Bluepring and the CME template for the autoprovision to succeed.

   - Enter the **Check Point Gateways Count** of Check Point Network Security Gateways to deploy on the AHV cluster. A single gateway is deployed on each AHV node based on the number of nodes that are on the cluster.

8. To deploy the Calm application, review the settings, and then click **Create**.

9. Verify the status of the deployment in the Nutanix Calm Applications Overview, use the **Audit** tab, to monitor the progress.

When the deployment finishes, the status changes from **Provisioning** to **Running**.

For more options, see the Nutanix Calm Administration and Operations Guide for your version.

**Note** - The Nutanix Calm Blueprint automatically creates the Check Point Service Chain **CPOS_CHAIN**.

These parameters are hard coded in the Nutanix Calm blueprint:

- **Service Name** - Check Point
- **Name** - Check Point Network Security Gateway
- **Cloud** - Nutanix
- **Operating System** - Linux
- **Boot Configuration** - Legacy Bios

**VM Configuration**

- **VM Name** - Check_Point_@@(cp_gw_version)@@_GW-@@(NUM)@@.

The names of the Virtual Machines are dynamically created based on the value defined in the VM Configuration section.

The default text Check_Point_@@(cp_gw_version)@@_GW-@@(NUM)@@ creates a Virtual Machines in this format:
Check_Point_R81_GW-1
Check_Point_R81_GW-2
....
Check_Point_R81_GW-x

**Note** – The name must contain the version of the CloudGuard Network Security Gateway for correct Autoprovision with the Cloud Management Extension (CME) utility, therefore this is mandatory: “._@@(#p_gw_version)@@_”.

- vCPU - 2
- Cores per vCPU - 2
- Memory (GiB) - 8

The Guest Customization checkbox is selected by default.

- **Cloud-init Type script**
  Contains some important configuration parameters for the Bridge and Firewall.

  **Important** - The Bridge interface must not be used, edited, or configured in any way. Any changes in the Bridge interface will have an impact on the Security Gateway's functionality.

  **Important** - Do not change or remove any lines from the Cloud-init script. This causes the CloudGuard Security Gateway to stop.

- **Boot Configuration – Legacy Bios**

**Disks**

- **Type** – Disk
- **Bus Type** – SCSI
- **Operation** – Clone from Image Service
- **Image** – CloudGuard Network Security Image uploaded to Prism Central in STEP 3.

**Categories**

- **network_function_provider: Check_Point** – Keep the value empty.

**Network Adapters (NICS)** – by default there are three NICs:

- **NIC 1** – CloudGuard Network Security Gateway Management interface
- **NIC 2** – Ingress bridge interface
- **NIC 3** – Egress bridge interface

**Serial Ports** - **Connected** checkbox must be selected by default. Do not clear the checkbox, this may cause large delays in the quantity of time it takes for instances to boot.

**Connection**

- **Credential** – admin
- **Address** – NIC 1
- **Connection type** – SSH
- **Connection Port** – 22
- **Delay (in seconds)** – 400. This allows the guest customization script to complete before it requests the check login script.
Note - If the Nutanix AHV operate in high use rates, it may be necessary to increase the default value from 400 to a larger value. An increase in the timeout value does not negatively affect the deployment of CloudGuard Network Security Gateways.

- **Retries** – 5. The number of login attempts if there is a login failure.

### Step 6: Apply Micro-Segmentation Policy Assignment

Nutanix Flow delivers advanced networking and security services, provides visibility into the virtual network, application-centric protection from network threats, and automation of common networking operations.

For more information about how to use the Nutanix Security Policy, see the [Nutanix Flow Security Policy Configuration](#) guide.

### Service Chain Insertion

Each defined flow in an application policy can be directed through a service chain when a chain exists. Service chains define a set of CloudGuard network function security gateways for advanced traffic processing. The deployment workflow for the CloudGuard Network Security Gateways and the creation of the service chain is automated directly from the Nutanix Calm Blueprint.

When the service chain is created, it is immediately available to use in the Flow right away. In Nutanix Prism Central, use Flow to create the allowed inbound or outbound rule, and then select a service chain.

### Configure Nutanix Flow to Route Traffic through the Service Chain

This option requires Nutanix Flow licenses for all AHV nodes that run CloudGuard Network Security Gateways in the targeted clusters. Before you start this configuration, you must enable Nutanix Flow micro-segmentation.

For more information, see [Nutanix Flow](#).

**Note** – There are many options to create a Security Policy. Here we give an example to emphasize how to redirect all the traffic in the AHV hosts in the cluster to the Check Point service chain `CPOS_CHAIN` and into the CloudGuard Network Security Gateways.

#### To apply the micro-segmentation policy:

1. Open the Nutanix Prism Central Web UI.
2. In Prism Central, select **Virtual Infrastructure > Categories > AppType > Update**.
   a. Create a new AppType category in Prism Central for the VM or VMs that are to redirect the traffic to the CloudGuard Network Security Gateway.
   b. Click **Save**.

   Assign the category to the VM or VMs that are to redirect the traffic to the CloudGuard Network Security Gateway.

3. In Prism Central, select **Virtual Infrastructure > VMs**.
   a. Select the checkbox next to the VM that you want to assign the category.
   b. Click **Actions > Manage Categories**
   c. Add the category that you created in this section.
Create Inbound and Outbound rules to direct the traffic through the Check Point Service Chain Create an Application Security Policy for the AppType Category created in this section.

1. Click **Create Security Policy > Secure applications (App Policy) > Create.**
2. Enter a **Name** and **Description** for the new Security Policy.
   a. In **Secure This App** list, select the AppType created in this section.
   b. Click **Next.**
3. Change the **Inbounds** and **Outbounds** rules to **Allowed List Only.**

**Create Inbound and Outbound rules to direct the traffic through the Check Point Service Chain**

1. Add source and destination by **Subnet/IP.**
   a. Add the source and destination IP as 0.0.0.0/0 to specify all sources and all destinations.
   b. Click **Add.**
2. After you add the source to connect the source and specify ports, click the blue plus sign on the **AppType:<...>**.
3. Enter a **Description:**
   a. In **Service Details > Allow all traffic.**
   b. Click the checkbox next to **Redirect through a service chain** and select the CPOS_CHAIN.
   c. Click **Save.**
4. Do step 1-2 again in this section for the outbound side > and then click **Next.**
5. Review the policy > click **Save and Monitor.**

(Optional) Deploy additional CloudGuard Network Security Gateways with Nutanix Calm Scale Out

The Scale-In and Scale-Out functionality allows the ability to increase or decrease the number of CloudGuard Network Gateways. When more Nutanix AHV cluster node are added to the environment, the Nutanix Scale-Out function provides a form in which more CloudGuard Network Security Gateway instances can be added to an existing deployment.

**To deploy more CloudGuard Network Security Gateways:**

1. Open the Nutanix Prism Central Web UI.
2. In Prism Central, select **Services > Calm > Applications.**
3. Open the Check Point Network Security application created with the Nutanix Calm Blueprint.
4. Select the **Manage.**
5. To Scale-Out more CloudGuard Network Gateway instances, click the play ▶ button.
6. Adjust the number of new CloudGuard Network Gateway instances to deploy.

After these steps are complete, the CloudGuard Network Security Gateways are:

- Automatically provisioned to the Security Management with the Cloud Management Extension (CME)
- Automatically added to the Check Point CPOS_CHAIN service chain, and are deployed on the new Nutanix AHV nodes that were added to the Nutanix Cluster.

For more information, see Nutanix Calm Administration And Operations Guide.

**Enabling the CloudGuard Controller**

![Best Practice - To benefit from more CloudGuard features, we recommend to enable the CloudGuard Controller.](image)
For more information, see the *R81 CloudGuard Controller Administration Guide*. 
Troubleshooting and Best Practices

Nutanix CME Controller is not Deleted

**Symptom:** When you try to delete Nutanix controller, there is an error.

**Solution:** Make sure the Nutanix Prism Central is running. If it is not, then:

- The Nutanix Prism Central was deleted and no longer exists.
- The Nutanix Prism Central Thumbprint changed.
- To delete the Nutanix controller, run:

  ```
  autoprov_cfg delete controller NUTANIX -cn <CONTROLLER_NAME>
  ```

  **Note** - If this is the last controller in the environment, it will not be deleted. Use this procedure only after you removed all the services from the Nutanix Prism Central:

Nutanix CME Controller Fingerprint Mismatch

**Symptom:** For a procedure on the Nutanix CME controller there is an error: "fingerprint mismatch: <FINGERPRINT>"

**Solution:** The fingerprint of the Nutanix CME controller has changed. It is necessary to verify the correct fingerprint again and make sure that this changes was approved before you continue. If you are not sure why the Nutanix Prism Central fingerprint changed, do not continue.

To update the Nutanix Prism Central Thumbprint, run:

  ```
  autoprov_cfg set controller NUTANIX -cn <CONTROLLER_NAME> -fn sha256:<FINGERPRINT>
  ```
Additional Resources

Check Point Software Technologies

- Check Point Software Technologies Support Site
- Check Point R81
- CloudGuard for Private Cloud images
- *R81 CloudGuard Controller Administration Guide*, see "CloudGuard Central Licensing".

Nutanix

- Nutanix V3 Rest API - Overview
- Nutanix Calm V3.1 Rest API
- Nutanix Developer Portal
- How to create a service chain using Rest API