Check Point
SOFTWARE TECHNOLOGIES LTD.

10 April 2019

# CHECK POINT CLOUDGUARD IAAS HIGH AVAILABILITY FOR MICROSOFT AZURE

## R80.10 AND ABOVE

Deployment Guide



# 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/IaaS/WebAdminGuides/EN/CP_CloudGuard_IaaS_HighAvailability_for_Azure/html_frameset.htm.

Download the latest version of this document in PDF format http://downloads.checkpoint.com/dc/download.htm?ID=76966.

### 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 Check Point CloudGuard IaaS High Availability for Microsoft Azure R80.10 and above Deployment Guide.

### Revision History

| Date | Description |
|---|---|
| 10 April 2019 | Updated: Load Balancer Conditions (on page 29) |
| 21 March 2018 | Updated: Step 5: Configure Cluster Objects in SmartConsole (on page 23) |
| 07 March 2018 | Updated: Step 1: Deploy with a Template in Azure (on page 16) - added the "Availability Zones" parameter |
| 17 February 2018 | Improved formatting and document layout<br>Updated: Network Diagram (on page 10)<br>Updated: Traffic Flows (on page 15) |
| 07 February 2018 | Updated: Testing and Troubleshooting (on page 32) |
| 06 January 2018 | First release of this document |

# Contents

# Terms

***Active***

State of a Cluster Member that handles network connections that pass through the cluster. In a cluster deployment, only one Cluster Member is Active and can handle connections.

***Active Directory (AD)***

Microsoft® directory information service. Stores data about user, computer, and service identities for authentication and access.

***Availability Set***

A collection of Virtual Machines that are managed together to provide application redundancy and reliability. The use of an availability set ensures that during either a planned or unplanned maintenance event at least one Virtual Machine is available. (Description from the Microsoft Azure glossary).

***Azure Environment***

An Azure environment an independent deployment of Microsoft Azure, such as Azure Cloud for global Azure and Azure China Cloud for Azure operated by 21Vianet in China.

***Azure PowerShell***

A command-line interface to manage Azure services via a command line from Windows. (Description from the Microsoft Azure glossary)

***Check Point WatchDog***

A process that launches and monitors critical processes such as Check Point daemons on the local machine, and attempts to restart them if they fail.

***Cluster***

Two or more Security Gateways that work together in a redundant configuration - High Availability.

***Failover***

Also, Fail-over. Transferring of a control over traffic (packet filtering) from a Cluster Member that suffered a failure to another Cluster Member (based on internal cluster algorithms).

***Load Balancer***

A resource that distributes incoming traffic among computers in a network. In Azure, a load balancer distributes traffic to Virtual Machines defined in a load-balancer set. A Load Balancer can be Internet-facing, or it can be internal. (Description from the Microsoft Azure glossary)

***Resource***

An item that is part of your Azure solution. Each Azure service enables you to deploy different types of resources, such as databases or Virtual Machines. (Description from the Microsoft Azure glossary)

***Resource Group***

A container in Resource Manager that holds related resources for an application. The resource group can include all of the resources for an application, or only those resources that are logically grouped together. You can decide how you want to allocate resources to resource groups based on what makes the most sense for your organization.

***SmartConsole***

Check Point main GUI client used to create and manage the security policy.

***Standby***

State of a Cluster Member that is ready to be promoted to Active state (if the current Active Cluster Member fails). Applies only to ClusterXL High Availability Mode.

***Subnet***

A logical subdivision of an IP network.

***User Defined Routing (UDR)***

A route table or a set of rules to create network routes, so that your Virtual Machine

can handle the traffic between subnets and to the Internet.

### *Virtual Machine (VM)*

The software implementation of a physical computer that runs an operating system. Multiple Virtual Machines can run simultaneously on the same hardware. In Azure, Virtual Machines are available in a variety of sizes. (Definition from the Microsoft Azure glossary).

### *Virtual Network*

A network that provides connectivity between your Azure resources that is isolated from all other Azure tenants. An Azure VPN Gateway lets you establish connections between Virtual Networks and between a Virtual Network and an on-premises network. You can fully control the IP address blocks, DNS settings, Security Policies, and route tables within a Virtual Network. (Description from the Microsoft Azure glossary)

# Check Point CloudGuard IaaS High Availability for Azure

*In This Section:*



## Prerequisites

To set up your system most efficiently, you have to be familiar with these topics:

| Vendor | Topics |
|---|---|
| Microsoft Azure | • Virtual Networks<br>• Virtual Machines<br>• Load Balancers<br>• High Availability ports<br>• Public IP addresses<br>• User Defined Rules (UDR)<br>• Role Based Access Control (RBAC) |
| Check Point | • R80.10 and above<br>• Check Point with Microsoft Azure |

## Setting Up Check Point High Availability Clusters in Azure

A cluster is a group of Virtual Machines that work together in High Availability Mode. One Cluster Member is the Active, and the second Cluster Member is the Standby. The cluster fails over from the Active Cluster Member to the Standby Cluster Member when necessary.

- Cluster Members communicate to each other with unicast IP addresses.
- For inbound, outbound, and East-West traffic, Cluster Members rely on Azure Load Balancers to represent their external and internal Virtual IP addresses. Load Balancers only forward traffic to the Active Cluster Member.
- For VPN traffic, Cluster Members use API calls to Azure to communicate the failover from the Active Cluster Member. The Standby Cluster Member then promotes itself to Active.

  During cluster failover, the Standby Cluster Member associates the private and public cluster IP addresses of the Active Cluster Member with its external interface.

### Azure API authentication

To make API calls to Azure automatically, Cluster Members need Azure Active Directory credentials. Use the Role-Based Access Control (RBAC) to enable Active Directory.

The Check Point Security Management Server in the Azure Cloud, or on-premises, manages the Check Point Cluster Members.

### Azure Internal Load Balancer

The Internal Load Balancer deploys by default as part of the solution template. It is automatically configured to listen and forward any TCP or UDP traffic on its High Availability ports. The Internal Load Balancer gets an automatically assigned name: `backend-lb`.

Azure sends probes from the source IP address 168.63.129.16 to TCP port 8117 to monitor the health of the Check Point CloudGuard IaaS Security Gateways.

# Network

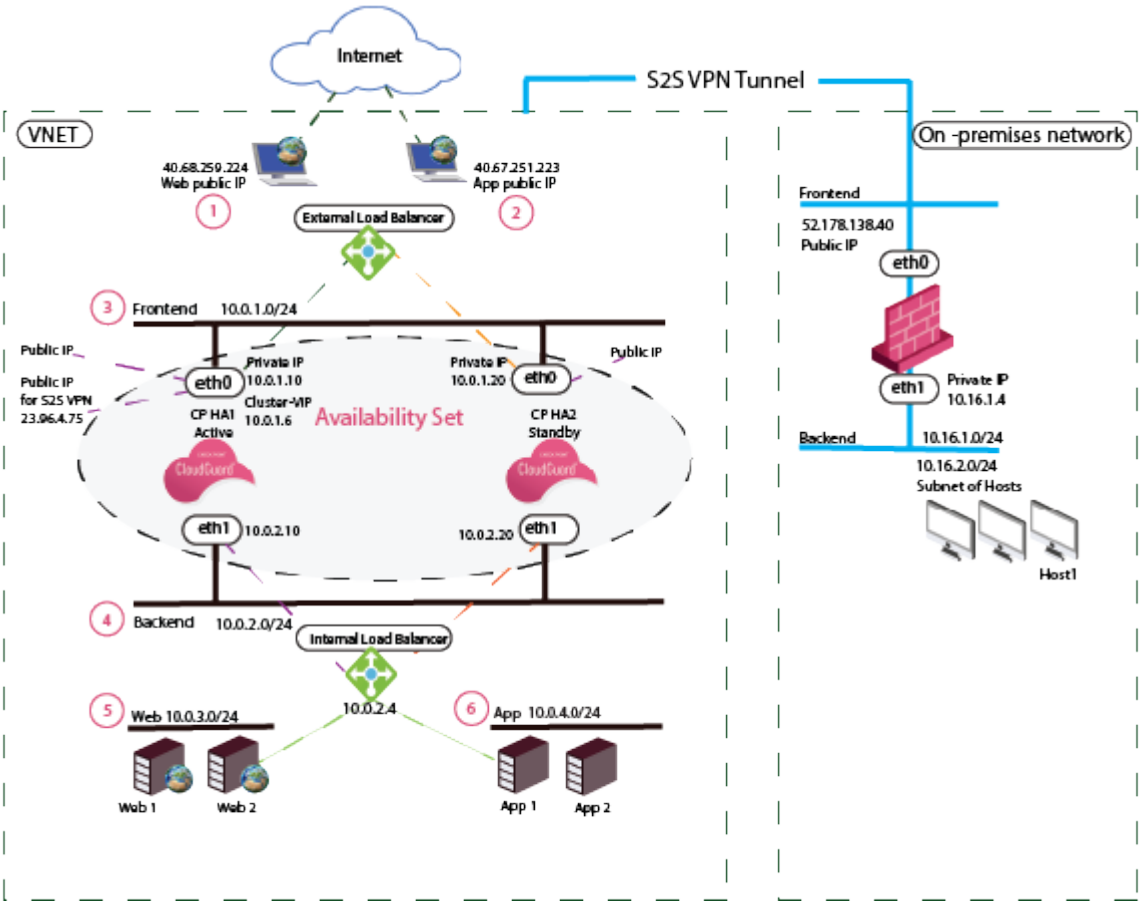
*In This Section:*



Follow this network diagram to configure your system. Make sure to replace the IP addresses in the sample environment with the IP addresses in your environment.

# Network Diagram

**See the routing tables below the diagram.**




## Load Balancing Rules of the External Load Balancer

| | | | |
|---|---|---|---|
| 1 | **Example 1** | **Frontend**<br>Web:443 | **Backend port**<br>8081 |
| 2 | **Example 2** | **Frontend**<br>App:80 | **Backend port**<br>8083 |

## Frontend Routing Table - User Defined Routes (UDR)

| | | |
|---|---|---|
| 3 | **Destination** | **Nexthop** |
| | 10.0.0.0/16 | None (Drop) |
| | 10.0.1.0/24 | Virtual Network |

## Backend Routing Table - User Defined Routes (UDR)

| | | |
|---|---|---|
| 4 | **Destination** | **Nexthop** |
| | 0.0.0.0/0 | None (Drop) |

## Routing Table for Web and App - User Defined Routes (UDR)

*Web and App routing tables have the same Virtual Network address, but different subnet addresses.*

**Web**

| | | |
|---|---|---|
| 5 | **Frontend** | **Nexthop** |
| | **10.0.0.0/16 -** *Virtual Network address* | **10.0.2.4 -** *IP of the Internal Load Balancer* |
| | **0.0.0.0/0** | **10.0.2.4 -** *IP of the Internal Load Balancer* |
| | **10.0.3.0/24** (Web) - *Subnet address* | Virtual Network |

**App**

| | | |
|---|---|---|
| 6 | **Frontend** | **Nexthop** |
| | **10.0.0.0/16 -** *Virtual Network address* | **10.0.2.4 -** *IP of the Internal Load Balancer* |
| | **0.0.0.0/0** | **10.0.2.4 -** *IP of the Internal Load Balancer* |
| | **10.0.4.0/24** (App) - *Subnet address* | Virtual Network |

# Diagram Components

**The diagram shows:**

- Virtual Network in Azure that is divided into four subnets
  - Frontend
  - Backend
  - Web
  - App
- On-premises network with these components
  - Security Gateway
  - Hosts

Check Point High Availability consists of two Cluster Members, Member 1 and Member 2. Each Cluster Member has two interfaces.

When the Cluster Members are in the same Availability Set, it guarantees that the two Cluster Members are in separate fault domains. For more information, see *Manage the availability of Windows virtual machines in Azure* https://docs.microsoft.com/en-us/azure/virtual-machines/windows/manage-availability?toc=%2Fazure%2Fvirtual-machines%2Fwindows%2Ftoc.json.

**In the diagram:**

- The cluster protects two web applications.
- There is Site-to-Site VPN connectivity between the Cluster Members and on-premises Security Gateways.

**Each web application has:**

- Public IP address
- Web server
- Application server

**You must manually configure these components:**

- Backend hosts
- Subnets
- Routing tables for Web and App servers

### Static IP Addresses:

| Name | Attached to | Use |
|---|---|---|
| Cluster public address | The external interface of the Active Cluster Member. | VPN |
| Cluster private address | The external interface of the Active Cluster Member. | VPN |
| Member 1 public address | The external interface of Member 1. | • External management of Member 1<br>• Internet and Azure API access<br>Do not disable or delete this resource. |
| Member 2 public address | The external interface of Member 2. | • External management of Member 2<br>• Internet and Azure API access<br>Do not disable or delete this resource. |
| Web | Azure Load Balancer | Public service Web |
| App | Azure Load Balancer | Public service App |

### Use the Azure Load Balancer rules to forward traffic that comes from the Internet:

**Note -** You cannot use these ports:

- 80
- 443
- 444
- 8082
- 8880
- 8117

Azure Load Balancer rules:

| Frontend IP address | Frontend TCP ports | Destination IP address | Destination port |
|---|---|---|---|
| Web | HTTPS | Active Cluster Member | 8081 |
| App | HTTP | Active Cluster Member | 8083 |

# Failover

This is what happens during cluster failover:

1. The Cluster Member that fails, immediately stops responding to the Load Balancer health probes.
2. The Cluster Member that gets promoted to Active, starts responding to the Load Balancer health probes.
3. The Azure External Load Balancer and Internal Load Balancer detect the new health status of each Cluster Member, and forward traffic to the healthy Cluster Member. For more information, see *Azure Load Balancer health probes* https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-custom-probe-overview.

   **This usually happens in less than 15 seconds** based on the health probe Load Balancer configuration. This affects inbound and East-West traffic inspection.
4. The Cluster Member that gets promoted to Active, uses the Azure API to associate itself with the cluster private and public IP addresses.

   **This usually happens in less than 2 minutes**. This affects VPN tunnel failover.

These are the expected failover times based on use case:

| Use Case | Expected Failover Time | Comments |
|---|---|---|
| Site-to-Site VPN | Less than 2 minutes | Depends on the Azure API. |
| Inbound inspection through the External Load Balancer | Less than 15 seconds | Depends on the Load Balancer health probe. |
| Outbound inspection through the Internal Load Balancer | Less than 2 minutes | Depends on the Load Balancer health probe and Azure API. |
| East-West inspection through the Internal Load Balancer | Less than 15 seconds | Depends on the Load Balancer health probe. |

# Traffic Flows

If the Management Server is in the Virtual Network, make sure to have specific routes to allow traffic between the Management Server Virtual Machine and the Cluster Members.

**Note** - No other Virtual Machines can be deployed in the Check Point solution subnets.

## Inbound Traffic

- Traffic travels into the External Load Balancer.
- The External Load Balancer forwards the traffic to the Active Cluster Member.
- The Active Cluster Member inspects the traffic, and forwards it to the destination.

## Inbound Traffic Reply

1. The traffic travels from the Web Server to the Internal Load Balancer.
2. The Internal Load Balancer forwards it to the Active Cluster Member.
3. The Active Cluster Member forwards it to the destination.

## Inbound VPN Traffic

1. Packet enters the frontend NIC of the Active Cluster Member.
2. The Active Cluster Member decrypts the packet.
3. The Active Cluster Member forwards the packet to its destination.

## Outbound Traffic

1. Traffic travels to an Internal Load Balancer based on the UDR.
2. The Internal Load Balancer forwards the traffic to the Active Cluster Member.
3. The Active Cluster Member inspects the traffic and forwards it to the destination.

## East-West Traffic

1. Traffic travels from one of the internal servers to the Internal Load Balancer of the Check Point solution.
2. The Internal Load Balancer forwards the traffic to the Active Cluster Member.
3. The Active Cluster Member forwards the traffic to the destination.

**Note** - The Internal Load Balancer deploys by default as part of the solution template and is automatically configured. It is configured to listen and forward any TCP or UDP traffic High Availability ports. It gets an automatically assigned name: `backend-lb`.

Azure sends probes from the source IP address 168.63.129.16 to TCP port 8117 to monitor the health of the Cluster Members.

## Intra-Subnet Traffic

Traffic travels freely in the subnet without inspection.

# Workflow for Setting Up a High Availability Cluster in Azure

*In This Section:*



## Step 1: Deploy with a Template in Azure

Deploy this solution through the Azure Portal. If you use a different environment than the Standard Azure environment, see *Using a Different Azure Cloud Environment* (on page 37).

- To access the Standard Azure environment, from the Azure Marketplace, see the Azure standard portal https://portal.azure.com/#create/checkpoint.vsecha.
- To access the Azure US Government environment, from the Azure Marketplace, see the Azure US Government portal https://portal.azure.us/#create/checkpoint.vsecha.

**Note -** Standard Load Balancers and High Availability ports are not available on the Azure Government Cloud environment.

When the template shows, enter information for these parameters:

| Parameter | Description |
|---|---|
| Cluster object name | Name of the cluster object resource group. |
| Credentials | Public key or user name and password for SSH connections to the Cluster Members. |
| Subscription | Azure subscription into which the cluster object is deployed. |
| Resource group | Azure resource group into which the cluster object is deployed. |
| Location | Location into which the cluster object is deployed. |
| License | Type of license:<br>• Bring your own license (BYOL)<br>• Pay as you go (PAYG) |
| Virtual Machine size | Size of each Virtual Machine instance in the cluster object. |
| SIC | SIC key to the Security Management Server. |

| Parameter | Description |
|---|---|
| Network setting | 1. Pre-existing Virtual Network and its subnets<br>2. Name of a new Virtual Network and subnets, into which the cluster object is deployed.<br>**Note** - When you use pre-existing subnets, make sure that:<br>• No other Virtual Machines are deployed in those subnets.<br>• Define UDRs properly for each subnet. See *Step 3: Set Up Internal Subnets and Route Tables* (on page 21).<br>• There is a Network Security Group (NSG) associated with your Frontend subnet to connect the External Load Balancer and Cluster Member. |
| Availability Zones | Use **Availability Set** (default) or **Azure Availability Zones** for your High Availability.<br>• First Cluster Member is be deployed in zone 1.<br>• Second Cluster Member is deployed in zone 2.<br>**Notes:**<br>• Only available if you deploy in a supported Azure location https://docs.microsoft.com/en-us/azure/availability-zones/az-overview#regions-that-support-availability-zones.<br>• Support for Azure Availability Zones is available with template version 20190303 and above. |

## Components of the Check Point Solution

**The Check Point deployed solution has these components:**

- Frontend subnet.

  The NSG is associated with the frontend subnet and allows all inbound and outbound TCP and UDP traffic.
- Backend subnet.
- Two Virtual Machines configured as a Check Point cluster.
- Internal Load Balancer.
- External Load Balancer.
- Public IP address for each Cluster Member.

No other Virtual Machines can be deployed in the solution's subnet.

**Notes about the template:**

- You can create a new Virtual Network, or deploy into an existing Virtual Network.
- Web and App subnets are not deployed automatically.
- It does not deploy any other Virtual Machines in the solution's frontend and backend subnets.
- Virtual Machines that are launched in the backend subnets, may require Internet access to finalize provisioning. Launch these Virtual Machines only after you have applied *Hide NAT* rules on the cluster object to support this type of connectivity.

- The Check Point First Time Configuration Wizard automatically deploys after you have set up the cluster object. The cluster object is configured based on the parameters you apply.
- After the First Time Configuration Wizard completes, the Virtual Machines automatically reboot.

**Important -** If you deploy the solution to an existing Virtual Network, confirm that there is an NSG associated with the frontend subnet that allows all inbound and outbound TCP and UDP traffic. An NSG is necessary to connect to Cluster Members successfully.

# Step 2: Set Credentials in Azure

By default, the automatic service principal is deployed. If you want to create your own service principal, make sure you set credentials and assign privileges to necessary resources. Managed service identity for Virtual Machines is only available in the Azure Cloud environment.

If you deploy in other environments, you have to create your own service principal manually. See *Creating your Own Service Principal* (on page 19).

## Azure Credentials and the Automatic Service Principal

The Check Point cluster template automatically creates a service principal for each Virtual Machine, and assigns a Contributor role to the cluster resource group. Therefore, there is no need to create a service principal, assign it a role, and attach it to each of your individual cluster resources. For more information, see *What is managed identities for Azure resources?* https://docs.microsoft.com/en-us/azure/active-directory/managed-service-identity/overview

After you deploy a Check Point cluster, the automatic credentials can be found in **Azure Portal > Resource groups > <cluster_resource_group > Access control (IAM)**. There are two service principals for each Cluster Member, each with a Contributor role.

**Notes:**

- If you delete the Cluster Member's Virtual Machine, the credentials are also deleted.
- Service principals never expire.

## Creating Your Own Service Principal

See *How to: Use the portal to create an Azure AD application and service principal that can access resources* https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal.

Use these parameters:

| Field | Parameter |
|---|---|
| Name | <*Application_Name*><br>Example: `check-point-`<*cluster*> |
| Application type | Web-App / API |
| Sign-on URL | `https://localhost/`<*Application_Name*><br>Example: `https:/localhost/check-point-`<*cluster*> |

After you create the application, write down these values:

- ApplicationId
  `client_id`
- Key Value
  `client_secret`
- Tenant ID (Directory ID)
  `tenant`

**Best Practice -** We recommend that you set the key to never expire. Go to your resource.

### To create a service principal:

| Step | Description |
|---|---|
| 1 | Click **Access control (IAM) > Add**. |
| 2 | Select your role. |
| 3 | Select your AD application. |
| 4 | Click **Save**. |
| 5 | Set the `client_id` and `client_secret` on each of the Cluster Members.<br>From Expert Mode, run this command on each Cluster Member:<br>`# azure-ha-conf --client-id '<ApplicationId>' --client-secret '<Key Value>' --force`<br>Example:<br>`# azure-ha-conf --client-id '5c1896fe-26b6-4a5b-8c81-34ae07c09a24' --client-secret '2G6E_\|]Y&\|@Il(L}-O>g' --force`<br>Note - Use single quotes to avoid shell expansion. |
| 6 | Make sure the file syntax is correct. From Expert Mode, run this command on each Cluster Member:<br>`# python -m json.tool $FWDIR/conf/azure-ha.json` |
| 7 | Reload the cluster Azure configuration. From Expert Mode, run this command on each Cluster Member:<br>`# $FWDIR/scripts/azure_ha_cli.py reconf` |

### To revert to your previous automatic credentials:

| Step | Description |
|---|---|
| 1 | Remove your service principal. |
| 2 | From Expert Mode, run this command on each Cluster Member:<br>`# azure-ha-conf --system-assigned --force` |
| 3 | Assign the two service principals to each resource and to Cluster Members.<br>For more information, see *Components of the Check Point Solution* (on page 17) > *Notes about the template*. |
| 4 | The service principal deploys automatically.<br>If you want to create a new service principal, assign the privileges to the necessary resources and to Cluster Members.<br>For more information, see *Manage access using RBAC and the Azure portal* https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal. |

# Step 3: Set Up Internal Subnets and Route Tables

You can use the Azure portal or the CLI to add internal subnets. Let's add the Web and App subnets to our Virtual Network.

For each internal subnet, you have to create an Azure routing table with these UDRs:

**Web Route Table**

| # | **Name** | **Address prefix** | **Nexthop-type** | **Nexthop-address** |
|---|---|---|---|---|
| 1 | <*web-subnet*>-local | *<10.0.3.0/24>* | Virtual Network | - |
| 2 | web-subnet-to-other-subnets | 10.0.0.0/16 | Virtual appliance | ILB-internal-address 10.0.2.4 |
| 3 | web-subnet-default | 0.0.0.0/0 | Virtual appliance | ILB-internal-address 10.0.2.4 |

**App Route Table**

| # | **Name** | **Address prefix** | **Nexthop-type** | **Nexthop-address** |
|---|---|---|---|---|
| 1 | <*app-subnet*>-local | 10.0.4.0/24 | Virtual Network | |
| 2 | *<app-subnet-to-other-subnets>* | *<10.0.0.0/16>* | Virtual appliance | ILB-internal-address 10.0.2.4 |
| 3 | app-subnet-default | 0.0.0.0/0 | Virtual appliance | ILB-internal-address 10.0.2.4 |

**Note** - If traffic inspection is required inside the Web/App subnets, override Rule 1 in the route tables above, <*web-subnet*>-local, and <*app-subnet*>-local.

**Important -** Associate the newly created routing table with the subnet to which it belongs.

If the subnet houses the Security Management Server that manages the Cluster Members, add these routes below as well. This allows the Security Management Server to communicate directly with each Cluster Member, without passing through the Active Cluster Member.

For example:

| **Name** | **Address-prefix** | **Nexthop type** | **Nexthop address** |
|---|---|---|---|
| `Subnet-name-cluster_member1-management` | `cluster_member1-internal-address/32`<br>*<10.0.2.10/32>* | `Virtual appliance` | `cluster_member1-internal address`<br>*<10.0.2.10>* |
| `Subnet-name-cluster_member2-management` | `cluster_member2-internal-address/32`<br>*<10.0.2.20/32>* | `Virtual appliance` | `cluster_member2-internal address`<br>*<10.0.2.20>* |

# Step 4: Set Up Routes on Cluster Members to the Internal Subnets

| Step | Description |
|---|---|
| 1 | Connect over SSH to each of the Cluster Members. |
| 2 | Log in to Gaia Clish, or Expert mode. |
| 3 | Add this route:<br>• In Gaia Clish, run these two commands:<br>`set static-route <Virtual-Network-IP-address/Prefix> nexthop gateway address <eth1-router-IP-address> on`<br>`save config`<br>• In Expert mode, run this command:<br>`clish -c 'set static-route <Virtual-Network-IP-address/Prefix> nexthop gateway address <eth1-router-IP-address> on' -s`<br>Example:<br>`set static-route 10.0.0.0/16 nexthop gateway address 10.0.2.1 on` |

**Parameters:**

| Parameter | Description |
|---|---|
| *<Virtual-Network-IP-address/Prefix>* | Specifies the prefix of the entire Virtual Network.<br>Example: 10.0.0.0/16 |
| *<eth1-router-IP-address>* | Specifies the first unicast IP address on the subnet, to which the `eth1` is connected.<br>Example: 10.0.2.1 |

**Notes:**

- If the Virtual Network comprises several non-contiguous address prefixes, repeat the command for each prefix.
- For vNET Peering:
  - Add a compatible route on each peer network.
  - Add the route for vNET Peering to each Cluster Member.

# Step 5: Configure Cluster Objects in SmartConsole

| Step | Description |
|---|---|
| 1 | Click the **Objects** menu **> More object types > Network Object > Gateways and Servers > Cluster > New Cluster**. |
| 2 | Select **Wizard Mode**.<br>The **Check Point Installed Gateway Cluster wizard** window shows. |
| 3 | Enter a **Cluster Name**.<br>Example: `checkpoint-cluster` |
| 4 | In the **Cluster IPv4 Address** field, enter the public address allocated for the cluster.<br>Note - You can find the cluster IP address in the Azure portal when you select the Active Cluster Member's primary **NIC > IP configuration > "cluster-vip"**. |
| 5 | Click **Next**.<br>The **Gateway Cluster Properties** window shows. |
| 6 | Click **Add**.<br>a) In the **Name** field, enter the first Cluster Member name.<br>Example: `member1`<br>b) In the **IPv4 address** field:<br>If you are managing the cluster from the same Virtual Network, enter the Cluster Member's private IP address.<br>Otherwise, enter the Cluster Member's public IP address.<br>c) In the **Activation Key** field, enter the SIC key you set up in Azure.<br>d) In the **Confirm Activation Key** field, enter the SIC key again.<br>e) Click **Initialize**.<br>If the Activation Key is confirmed, the **Trust State** field shows **Trust Established**.<br>f) Click OK. |
| 7 | Repeat the Step 6 to add the second Cluster Member. |
| 8 | Click **Next**.<br>The **Cluster Topology** window shows. |
| 9 | Select **Cluster Synchronization > Primary > Next**. |
| 10 | Select **Cluster Synchronization > Secondary > Next**. |
| 11 | Select **Edit Cluster's Properties > Finish**. |

| Step | Description |
|---|---|
| 12 | Review the cluster settings.<br>Configure the interfaces **eth0** and **eth1**.<br>a) Select **Network Management**.<br>b) Double-click the interface **eth0**.<br>The **Network eth0** window shows.<br>c) From the **General** tab, in the **Network type** field, select **Cluster + Sync**.<br>d) In the **Virtual IPv4** field, enter the private VIP address and subnet mask of the cluster.<br>In the diagram, the private VIP address is: 10.0.1.6<br>**Note -** You can find the cluster private VIP address in the Azure portal when you select the Active Cluster Member primary **NIC > IP configuration > "cluster-vip"**.<br>e) From the **Network eth0** window, click **Topology** and disable the Anti-Spoofing.<br>f) Click **OK**.<br>g) Double-click the interface **eth1**.<br>The **Network eth1** window shows.<br>h) From the **Network eth1** window, click **Topology** and disable the Anti-Spoofing.<br>i) Click **OK**. |
| 13 | Install the applicable Access Control Policy on the cluster object. |

# Step 6: Configure NAT Rules

Note - See *Creating Objects in SmartConsole* (on page 40).

In SmartConsole, create the NAT rules below to provide Internet connectivity from the internal subnets:

| No | Original Source | Original Destination | Original Services | Translated Source | Translated Destination | Translated Services | Install On | Comments |
|---|---|---|---|---|---|---|---|---|
| **1** | Virtual Network | Virtual Network | *Any | = Original | = Original | = Original | Cluster object | Avoid NAT in the Virtual Network |
| **2** | App-subnet | App-subnet | *Any | = Original | = Original | = Original | Cluster object | |
| **3** | App-subnet | *Any | *Any | App-subnet (hidden address) | = Original | = Original | Cluster object | |
| **4** | Web-subnet | Web-subnet | *Any | = Original | = Original | = Original | Cluster object | |
| **5** | Web-subnet | *Any | *Any | Web-subnet (hidden address) | = Original | = Original | Cluster object | |

**Notes about the NAT rules:**

- Rule 1 - You have to define this NAT rule *manually*.
- Rules 2 - 5 - SmartConsole creates these NAT rules *automatically*.
- Traffic between the *Web-subnet* and the *App-subnet* is based on the UDR rules. Each subnet has its own routing table.

### For each internal subnet, create a network object:

| Step | Description |
|---|---|
| 1 | Double-click the Web-subnet object.<br>The **Web-subnet object** window shows. |
| 2 | Select the **NAT** tab **> Add automatic address translation rules**. |
| 3 | In the **Translation method** field, select **Hide > Hide Behind Gateway**. |
| 4 | In the **Install on Gateway** field, select the cluster object. |
| 5 | Click **OK**.<br>This creates the *automatic* NAT rules. |
| 6 | Install the applicable Access Control Policy on the cluster object. |

# Step 7: Set Up the External Load Balancer in Azure

By default, the template you deploy creates an External Load Balancer, with the name `frontend-lb`, which faces the Internet.

The External Load Balancer sends health probes to TCP port 8117 to determine the health of the CloudGuard IaaS Security Gateways.

Create the load balancing rules in the Azure portal to allow incoming connections:

| Step | Description |
|---|---|
| 1 | Go to **External Load Balancer > Frontend IP configuration**. |
| 2 | Click **Add**. |

**Notes:**

- You cannot use these ports for forwarded traffic:
  - 80
  - 443
  - 444
  - 8082
  - 8080
  - 8117
- Do not change the health probe port.
- The Check Point cluster resource group includes an NSG associated with the frontend subnet. By default, the NSG allows all outbound and inbound traffic.
- The Load Balancer can be set up to listen on additional ports or on additional public IP addresses.

For more information, see *Multiple Frontends for Azure Load Balancer* https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-multivip-overview. For an example, go to *Step 9: Configure the Load Balancer to Listen on Multiple IP Addresses in Azure* (on page 28).

# Step 8: Create Dynamic Object LocalGatewayExternal in SmartConsole

In SmartConsole, create the Dynamic object called *LocalGatewayExtenal*.

This object represents the private Cluster Member's IP addresses.

You use this Dynamic object in the next step.

| Step | Description |
|---|---|
| 1 | In SmartConsole, click the **Objects** menu **> Object Explorer**. |
| 2 | From the top toolbar, click **New > Network Object > Dynamic Objects > Dynamic Object**. |
| 3 | In the **Enter Object Name** field, enter (case-sensitive):<br>`LocalGatewayExternal` |
| 4 | Click **OK**. |
| 5 | Close the **Object Explorer**. |

# Step 9: Configure the Load Balancer to Listen on Multiple IP Addresses in Azure

Configure the Load Balancer to listen on additional public IP addresses. This setup is useful if you want the Security Gateway to secure multiple web applications, each with its own public IP address.

Configure the Load Balancer to listen on a second public IP address on TCP port 80, and then forward the traffic to the Check Point CloudGuard Security Gateway to TCP port 8083.

**To configure the frontend pool:**

| Step | Description |
|---|---|
| 1 | In the Azure portal, select the Load Balancer called `frontend-lb`.<br>**Note** - The Load Balancer is in the resource group you created. |
| 2 | Allocate a new public IP address:<br>a) Click **Frontend IP configuration** > **Add**.<br>b) Select a **Name**.<br>**Example:** <*cluster*>`-app-2`<br>c) Select the public **IP address** you created.<br>d) Click **OK**. |
| 3 | Add a load balancing rule.<br>a) Click **Load balancing rules** > **Add**.<br>b) Enter the rule name.<br>**Example:** <*cluster*>`-app-2-tcp-80`<br>c) In the **Frontend IP address** field, select the newly created Frontend IP address.<br>d) In the **Protocol** field, select **TCP**.<br>e) In the **Port** field, enter 80.<br>f) In the **Backend port** field, enter 8083.<br>g) In the next **Backend pool** field, select the pre-existing cluster pool.<br>h) In the **Health probe** field, select the health probe created by default by the template (TCP, port 8117).<br>i) In the **Session persistence** field, select **None**.<br>j) Set the desired **Idle timeout**, in minutes.<br>k) In the **Floating IP** field, select **Disabled**.<br>l) Click **OK**. |

## Load Balancer Conditions

The Active Cluster Member uses NAT to forward traffic that belongs to the two web applications, to the appropriate web server.

NAT rules are defined with the special Dynamic Object.

The Dynamic object `LocalGatewayExternal` represents the private IP addresses of the external interface of Member 1 and Member 2.

For more information, see *Step 8: Create Dynamic Object LocalGatewayExternal in SmartConsole* (on page 27).

| No | Original Source | Original Destination | Original Services | Translated Source | Translated Destination | Translated Services | Install On |
|---|---|---|---|---|---|---|---|
| 1 | *Any | LocalGatewayExternal | TCP 8081 | = Original | s App | https | Policy Targets |
| 2 | *Any | LocalGatewayExternal | TCP 8083 | = Original | s Web | https | Policy Targets |

# Step 10: Configure VPN

In SmartConsole, create a Network Group object to represent the encryption domain for the cluster.

To create an object for the VPN configuration, see *Creating Objects in SmartConsole* (on page 40).

For more information, see the *Check Point Security Management Administration Guide* for your Management Server version (for example: *R80.10* https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_SecurityManagement_AdminGuide/html_frameset.htm, *R80.20* https://sc1.checkpoint.com/documents/R80.20_GA/WebAdminGuides/EN/CP_R80.20_SecurityManagement_AdminGuide/html_frameset.htm).

| Step | Description |
|---|---|
| 1 | Create a Network Group object to represent the encryption domain of the cluster:<br>1. In SmartConsole, click the **Objects** menu > **Object Explorer**.<br>2. From the top toolbar, click **New > Network Group**.<br>3. In the **Enter Object Name** field, enter the desired name.<br>4. Click the **+** icon and select the applicable network objects.<br>5. Click **OK**.<br>6. Close the **Object Explorer**. |
| 2 | Edit the cluster object:<br>1. In SmartConsole, from the left navigation panel, click **Gateways & Servers**.<br>2. Double-click the cluster object.<br>The **Gateway Cluster Properties** window shows. |
| 3 | Define your Network Group as the encryption domain of the cluster object:<br>1. In SmartConsole, from the left navigation panel, click **Gateways & Servers**.<br>2. Double-click the cluster object.<br>The **Gateway Cluster Properties** window shows.<br>3. In the cluster object left tree, click **Network Management > VPN Domain.**<br>4. Select **Manually defined**.<br>5. In the right corner of this field, click the **[...]** button and select the Network Group object you created in Step 1. |
| 4 | Define the VPN community:<br>1. In the cluster object left tree, click **IPsec VPN**.<br>2. In the section **This Security Gateway participates in the following VPN Communities**, select the applicable VPN community. |

| Step | Description |
|---|---|
| 5 | Define the outgoing VPN interface:<br>1. In the cluster object left tree, click **IPsec VPN > Link Selection**.<br>2. In the **IP Selection by Remote Peer** section, select **Always use this IP address > Main address**.<br>3. In the **Outgoing Route Selection** section:<br>a) Click **Source IP address settings**<br>b) Select **Manual**<br>c) Select **Selected address from topology table.**<br>d) Select the private cluster object VIP address.<br>e) Click **OK**.<br>4. In the **Tracking** section, select the desired option.<br>5. Click **OK** to close the **Gateway Cluster Properties** window. |
| 6 | Configure the VPN Community to use Permanent Tunnels:<br>1. In SmartConsole, click the **Objects** menu > **Object Explorer**.<br>2. In the left tree, clear all boxes except for **VPN Communities**.<br>3. Double-click the VPN community, in which this cluster object participates.<br>The **VPN Community** window shows.<br>4. In the left tree, click **Tunnel Management**.<br>5. Select **Set Permanent Tunnels**.<br>6. Select the applicable option.<br>7. Click **OK** to close the VPN Community properties window.<br>8. Close the **Object Explorer**. |
| 7 | Install the applicable Access Control Policy on the cluster object. |

# Additional Information

*In This Section:*



## Testing and Troubleshooting

You can use the APIs to retrieve information about the cluster resource group.

**Use these commands on each Cluster Member to confirm that the cluster operates correctly:**

Note - Run these commands from Gaia Clish, or the Expert Mode.

```
cphaprob state
cphaprob -a if
```

Example:

```
[Expert@HostName:0]# cphaprob state
Cluster Mode:   High Availability (Active Up) with IGMP Membership
Number     Unique Address  Assigned Load   State
1 (local)   10.0.1.10       0%             Active
2           10.0.1.20       100%           Standby
```

**Use the cluster configuration test script on each Cluster Member to confirm it is configured correctly:**

**The script verifies:**

- The configuration file is defined in `$FWDIR/conf/azure-ha.json`. This file is created by the ARM template.
- A Primary DNS server is configured and works.
- The machine is set up as a Cluster Member.
- IP forwarding is enabled on all network interfaces of the Cluster Member.
- It is possible to use the APIs to retrieve information about the cluster's resource group.
- It is possible to log in to Azure with the Azure credentials in the `$FWDIR/conf/azure-ha.json` file.
- Calibration of ClusterXL configuration for Azure.

**To get the latest version of the test script:**

Note - Perform Steps 2 - 8 on each Cluster Member.

1. Download the latest version of the test script http://supportcenter.checkpoint.com/file_download?id=81245.
2. Copy the download TGZ file to some directory.
3. Connect to the command line.
4. Log in to the Expert mode.
5. Unpack the TGZ file:
   ```
   # tar -zxvf /<path to the downloaded script package>/Azure_cluster_ha_testing_sk110194.tgz
   ```
6. Back up the current $FWDIR/scripts/azure_ha_test.py script:
   ```
   # mv -v $FWDIR/scripts/azure_ha_test.py{,_backup}
   ```
7. Copy the latest script to the `$FWDIR/scripts/` directory:
   ```
   # cp -v /<path to the downloaded script package>/azure_ha_test.py $FWDIR/scripts/
   ```
8. Assign the required permissions:
   ```
   # chmod -v 755 $FWDIR/scripts/azure_ha_test.py
   ```

**To run the script on each Cluster Member:**

1. Connect to the command line.
2. Log in to the Expert mode.
3. Run the script with this command (do not change the syntax):
   ```
   # $FWDIR/scripts/azure_ha_test.py
   ```
   If all tests were successful, this shows: `All tests were successful!`
   Otherwise, an error message is displayed with information to troubleshoot the problem.

**A list of common configuration errors:**

| Message | Recommendation |
|---|---|
| `The attribute (ATTRIBUTE) is missing in the configuration` | |
| `Primary DNS server is not configured` `Failed to resolve (host)` | The Cluster Member is not configured with a DNS server. |
| `Failed in DNS resolving test` | Confirm that DNS resolution on the Cluster Member works. |
| `You do not seem to have a valid cluster configuration` | Make sure that the Cluster Member configuration on the Check Point Security Management Server is complete and that the Security Policy is installed. |
| `IP forwarding is not enabled on Interface (Interface-name)` | Use PowerShell to enable IP forwarding on all the network interfaces of the Cluster Member. |
| `failed to read configuration file: /opt/CPsuite-R80/fw1/conf/azure-ha.json` | The Azure Cluster Member configuration is not up to date, or written correctly. |
| `Testing credentials` | Failed to log in with the credentials provided. See the exception text to understand why. |
| `Testing authorization (Exception)` | Make sure the Azure Active Directory service account you created is designated as a Contributor to the cluster resource group. |

### Simulate a cluster failover:

For example, shut down the internal interface of the Active Cluster Member.

1. On the current Active Cluster Member, run from the Expert Mode:
   ```
   # ip link set dev eth1 down
   ```
2. In a few seconds, the second Cluster Member has to report itself as the Active Cluster Member. Examine the cluster state on each Cluster Member. Run from Gaia Clish, or Expert Mode:
   ```
   cphaprob state
   ```
3. On the former Active Cluster Member, run from the Expert Mode:
   ```
   # ip link set dev eth1 up
   ```

### If you experience issues:

- Make sure you have a configured Azure Active Directory Service Account. The service has to have:
  - Contributor privileges to the resource group
  - At least minimum privileges on the Cluster Member deployment resources. See *Changing Template Components* (on page 39) > *Permissions*.
- To make the networking changes automatically, the Cluster Members have to communicate with Azure. This requires HTTPS connections over TCP port 443 to the Azure end points. Make sure the Security Policy that is installed on the Cluster Members allows this type of communication.

# Using the Azure High Availability Daemon

The cluster solution in Azure uses the daemon to make API calls to Azure when a cluster failover takes place. This daemon uses a configuration file `$FWDIR/conf/azure-ha.json` on each Cluster Member.

When you deploy the solution above from the template supplied, this file is created automatically.

The configuration file is in JSON format and contains these attributes:

| Attribute name | Type | Value |
|---|---|---|
| `debug` | Boolean | `true` or `false` |
| `subscriptionId` | String | Subscription ID. |
| `location` | String | Resource group location. |
| `environment` | String | Name of the environment. |
| `resourceGroup` | String | Resource group name. |
| `credentials` | String | IAM. Indicates using automatic credentials on the Cluster Member Virtual Machine. |
| `proxy` | String | Name of the proxy. |
| `virtualNetwork` | String | Name of the Virtual Network. |
| `clusterName` | String | Name of the cluster. |
| `templateName` | String | Name of the template. |
| `tenantId` | String | ID of the tenant. |

**Note -** If you use your own service principal, the `credentials` attribute contains:

- Your Client-ID
- Your Client-secret
- Grant type `client-credentials`
- Your Tenant ID

You can confirm that the daemon in charge of communicating with Azure runs on each Cluster Member. From Expert Mode, run:

```
# cpwd_admin list | grep -E "PID|AZURE_HAD"
```

The output should look like in this example:

```
APP        PID    STAT  #START  START_TIME             MON  COMMAND
AZURE_HAD  3663   E     1       [12:58:48] 15/1/2016   N    python
/opt/CPsuite-R80.20/fw1/scripts/azure_had.py
```

**Notes:**

- The script appears in the output:
  - The STAT column should show **E** (executing)
  - The #START column should show **1** (the number of times this script was started by the Check Point WatchDog)

To troubleshoot issues related to this daemon, generate debug. From Expert Mode, run:

- To enable debug printouts:
```
# azure-ha-conf --debug --force
```
- To disable debug printouts:
```
# azure-ha-conf --no-debug --force
```

The debug output is written to `$FWDIR/log/azure_had.elg*` files.

# Using a Different Azure Cloud Environment

If you want to deploy your cluster in an environment other than the standard Azure environment, make sure to edit this file:

`$FWDIR/conf/azure-ha.json`

Example:

```
{
...
    "environment": "[Azure-cloud-environment]",
...
}
```

The Azure-Cloud-Environment has to be one of these:

- Azure Cloud (the default global cloud environment)
- Azure China Cloud
- Azure US Government
- Azure German Cloud

**Procedure:**

| Step | Description |
|---|---|
| 1 | From Expert Mode, run:<br>`# azure-ha-conf --environment '<Azure-cloud-environment>' --force` |
| 2 | Make sure the file syntax is correct. From Expert Mode, run:<br>`# python -m json.tool $FWDIR/conf/azure-ha.json` |
| 3 | Apply the changes. From Expert Mode, run:<br>`# $FWDIR/scripts/azure_ha_cli.py reconf`<br>Note -If you deploy in the default global cloud environment, you can omit this attribute. |

**Important note about the service principal:**

If you use any of these different environments, you have to create your own service principal. No default service principal is created.

# Working with a Proxy

In some deployments, you can only access the Internet through a web proxy. To allow the Cluster Member to make API calls to Azure through the proxy, edit the `$FWDIR/conf/azure-ha.json` file and add this attribute:

```
{
...
    "proxy": "http://[proxy-name]:[proxy-port]",
...
}
```

- *proxy-name* is the host name or IP address of the web proxy server
- *proxy-port* is the port on the proxy server

**Note -** The URL scheme has to be HTTP and not HTTPS.

Example:

```
{
...
     "proxy": "http://proxy.example.com:8080",
...
}
```

**Procedure:**

| Step | Description |
|---|---|
| 1 | Change the proxy settings. From Expert Mode, run:<br>`# azure-ha-conf --proxy 'http://[proxy-server-ip-or-hostname]:[proxy-port]' --force` |
| 2 | Make sure the file syntax is correct. From Expert Mode, run:<br>`# python -m json.tool $FWDIR/conf/azure-ha.json` |
| 3 | Apply the changes. From Expert Mode, run:<br>`# $FWDIR/scripts/azure_ha_cli.py reconf` |

# Changing Template Components

The Check Point cluster's public IP address has to be in the same resource group as the Cluster Members.

### These resources can be in any resource group:

- Virtual Network
- Network interfaces
- Route tables
- Storage account

**Note** - Make sure the resources Virtual Network and External Network Interfaces use the same automatic service principal with the same permissions.

### Naming Constraints

- Cluster Members in Azure have to match the Cluster Member names with a suffix of '1' and '2'.
- The IP address of the cluster has to match the configuration file.
- By default it should match the cluster name.

### Permissions

It is possible to assign service principal permissions to specific Azure resources. See sk116585 http://supportcontent.checkpoint.com/solutions?id=sk116585 for information on how to find the image version.

To allow the cluster to update the necessary Azure resources on failover, the service principal has to be assigned at least these roles on these resources or on their respective resource group:

| Resource Type | Role |
|---|---|
| Any public IP address attached to the External Load Balancer | Virtual Machine contributor |
| Public Load Balancer | Network contributor |
| CloudGuard Virtual Machines | Reader |
| Cluster public IP address | Network contributor |
| Public IP address of each Cluster Member | Virtual Machine contributor |
| Virtual Network | Virtual Machine contributor |
| The external network interfaces (`eth0`) used by the Cluster Member | Virtual Machine contributor |

# Creating Objects in SmartConsole

For more information, see the *Check Point Security Management Administration Guide* for your Management Server version (for example: *R80.10* https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_SecurityManagement_AdminGuide/html_frameset.htm, *R80.20* https://sc1.checkpoint.com/documents/R80.20_GA/WebAdminGuides/EN/CP_R80.20_SecurityManagement_AdminGuide/html_frameset.htm).

**Important -** After you create an object, you must publish the session to save the changes in the management database.

### To create a Host object:

| Step | Description |
|---|---|
| 1 | From the top right **Objects Pane**, click **New > Host**.<br>The **New Host** window shows. |
| 2 | In the **Machine** field, enter the private IP address of the machine. |

### To create a Network object:

| Step | Description |
|---|---|
| 1 | From the top right **Objects Pane**, click **New > Network**.<br>The **New Network** window shows. |
| 2 | Enter the **Object Name** (specifically the subnet name). |
| 3 | Enter the **Network address** and **Net mask**. |

### To create a Service (port) object:

| Step | Description |
|---|---|
| 1 | From the top right **Objects Pane**, click **New > More > Service**. |
| 2 | Select your TCP/UDP service. |
| 3 | Enter the **Object name**. |
| 4 | In the **Enter Object Comment** field, enter the port name. |
| 5 | In the **General** field, select your **Protocol**. |
| 6 | In the **Match By** field, select the **Port** number. |
| 7 | Click **OK**. |

### To create a Network Group object:

| Step | Description |
|---|---|
| 1 | From the top right **Objects Pane**, click **New > Network Group**.<br>The **New Network Group** window shows. |
| 2 | Click **+** to select your internal subnets. |
| 3 | Click **OK**. |

# Related Solutions

- sk109360 - Check Point Reference Architecture for Azure
  http://supportcontent.checkpoint.com/solutions?id=sk109360
- sk113583 - How to add a network interface to a Check Point Security Gateway in Azure
  http://supportcontent.checkpoint.com/solutions?id=sk113583
- sk113476 - Azure Virtual Network peering
  http://supportcontent.checkpoint.com/solutions?id=sk113476

# Known Limitations

- Support for Jumbo Hotfix Accumulators:
  - For R80.20 High Availability deployment, there is no support yet for a Jumbo Hotfix Accumulator.
  - For R80.10 High Availability deployment, you can install R80.10 Jumbo Hotfix Accumulator (R80_10_jumbo_hf) - Take 135 and above only. See sk116380 http://supportcontent.checkpoint.com/solutions?id=sk116380.
- Only two Cluster Members in a cluster are supported.
- Only High Availability Mode (Active/Standby) is supported. Load Sharing Mode is not supported.
- VRRP cluster is not supported.
- Only the Active Cluster Member can reach services from the cluster through VPN.

  The Standby Cluster Member can reach those services only when it becomes the Active Cluster Member.
- For outbound and VPN traffic, you cannot delete or disable the public IP addresses of Cluster Members.
- The feature is only available in Azure Resource Manager deployments.

  It is not supported with Azure Service Manager (also known as classic) deployments.
- When you use the standard Internal Load Balancer it does not support Stateful failover.
- Managed service identity for Virtual Machines is only available in the Azure Cloud environment.

  Other environments require a manual service identity management.
- Standard Load Balancers and High Availability ports are not available on the Azure Government Cloud environment