

***Quick Deployment Guide for Virtual Machine
Scale Sets (VMSS) for Microsoft Azure with
Remote Access VPN***

R80.40 and Above

Quick Deployment Written Guide & Videos

August 26, 2020

Table of Contents

Overview	3
Prerequisites.....	3
Components of the Check Point Deployed Solution.....	4
Network Diagram.....	6
Remote Access VPN Solution: High Level Architectural Diagram:.....	7
Remote Access VPN.....	8
Configuration Steps	9
Step 1 Create an Azure AD and Service Principal	9
Step 2: Deploy the Azure App Service Domain	10
Step 3: Configure the Check Point Security Management Server	11
Step 4: Deploy the Check Point VMSS and Assign the Azure AD Application..	18
Step 5: Deploy the Azure Function Code	22
Step 6: Configure and Deploy the Remote Access VPN Client	24
Step 7: Create a Source NAT rule for Office mode ip address range network	25
Troubleshooting	26
Remote Access VPN.....	26
Known Limitations	27

Overview

Use this guide to:

- Deploy a new Check Point [VMSS](#)¹ for Microsoft Azure with Remote Access VPN

Prerequisites

Make sure you are familiar with these topics:

Vendor	Topics
Microsoft Azure	<ul style="list-style-type: none">▪ VMSS▪ Autoscaling▪ Load Balancers<ul style="list-style-type: none">• High Availability ports▪ Identity and access management▪ Azure Function▪ Azure DND
Check Point	<ul style="list-style-type: none">▪ Check Point R80.40 and Above▪ Check Point with Azure

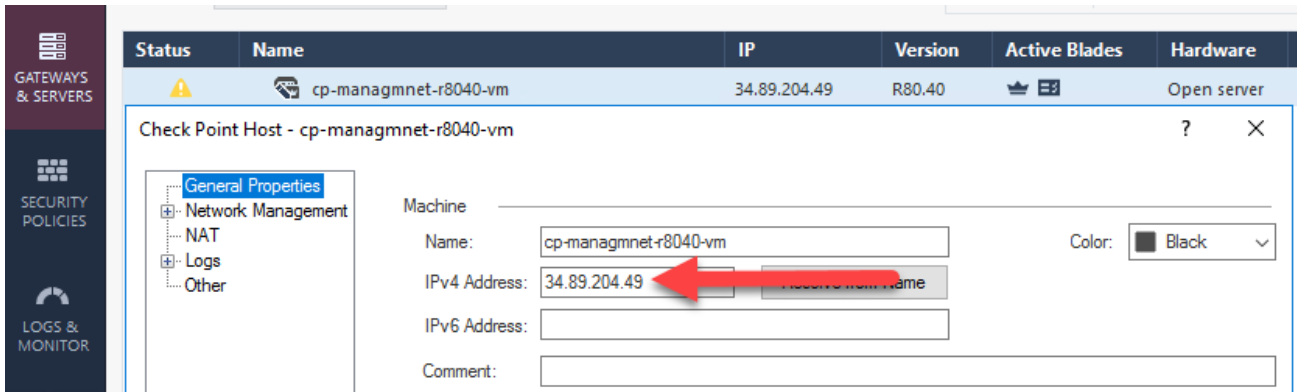
**** This guide does not cover the deployment of the Check Point management server. This guide assume that you already have a running management server.**

**** This guide assume that the VMSS CloudGuard gateways would be managed by the management server with the CloudGuard gateways public ip addresses (managed over the internet and not via VPN or Internal connection eg. Express route)**

**** The management server should have a static public ip address or a private ip address With a static NATed public ip address.**

**** The Check Point management server object in the SmarConsole Gateways & Servers Section should have it's public ip address in the main object ip address.**

¹ When you create an Azure virtual machine (VM), you must create a virtual network (VNet) or use an existing VNet. You also need to decide how your VMs are intended to be accessed on the VNet. It is important to plan before creating resources and make sure that you understand the limits of networking resources.



**** Only VPN Clients that you will find in this guide (page 24) support connection enhancement to VMSS CloudGuard Gateways.**

**** The Remote Access VPN is supported from CloudGuard Gateways R80.40 and above.**

Components of the Check Point Deployed Solution

The diagram below depicts an Azure Virtual Network (VNET) with the Check Point solution deployed. There are two backend vNets – Spoke-02 and Express-Route. Express-Route and Spoke-02 are each a user-deployed backend vNets & subnet. Spoke-02 has its own load-balanced web server.

A vNet peering is connecting between the CloudGuard vNet (Northboundhub) to the Spoke-02 and the Express-Route vNets.

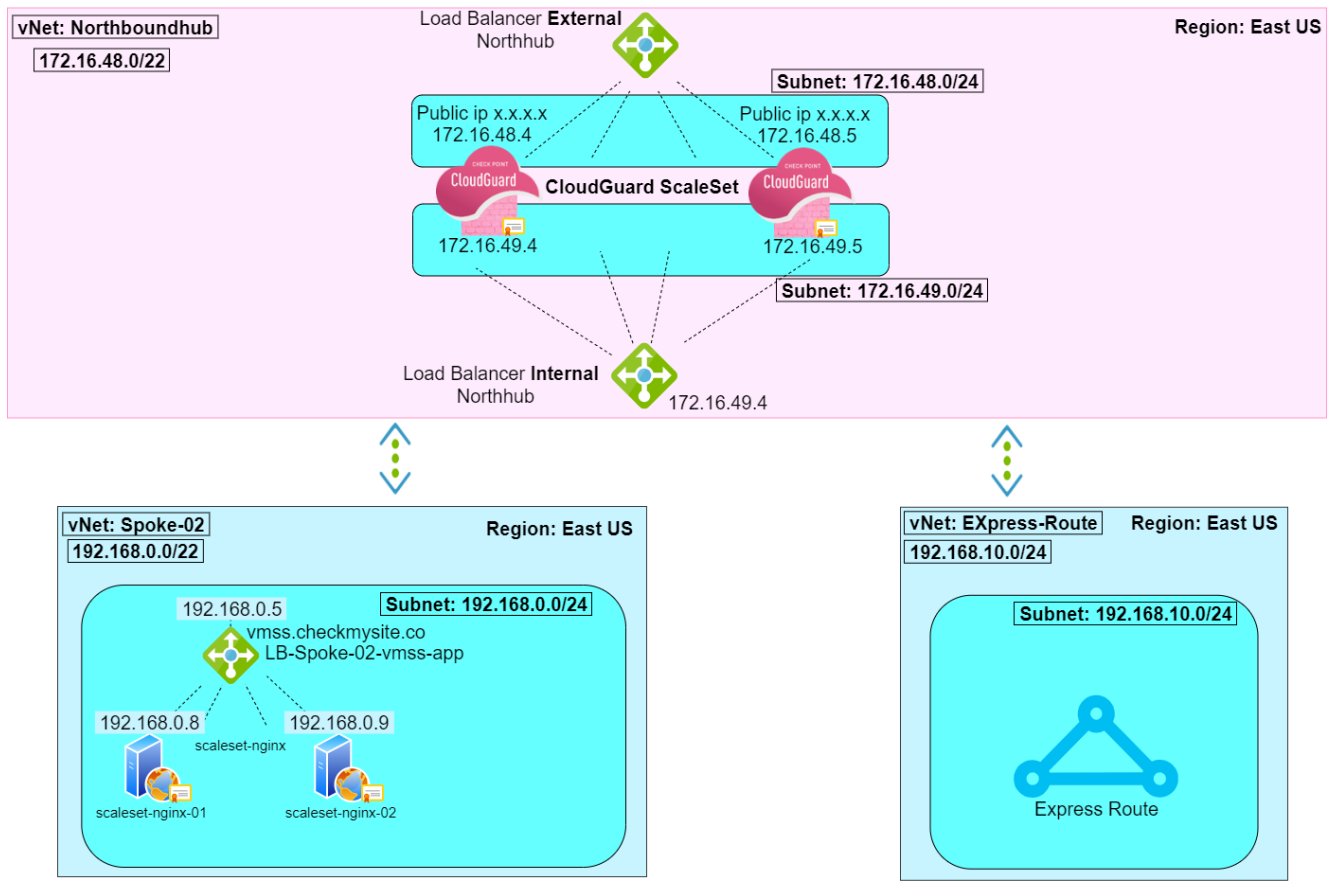
The Check Point **deployed solution has these components:**

- Dedicated Resource Group
- Dedicated vNet
- Frontend subnet & Backend Subnet
- Virtual Machine Scale Set (VMSS)
The number of instances that you can deploy in the Cloud is dynamic.
- Internal Load Balancer
- External Load Balancer (In case that you don't want to publish applications to the internet, there is no need to deploy an external load balancer, you will be able to deploy in anytime you want in the future in case you will need it)
- Public IP address for each VMSS instance
- You cannot deploy other VMs in the VMSS subnets

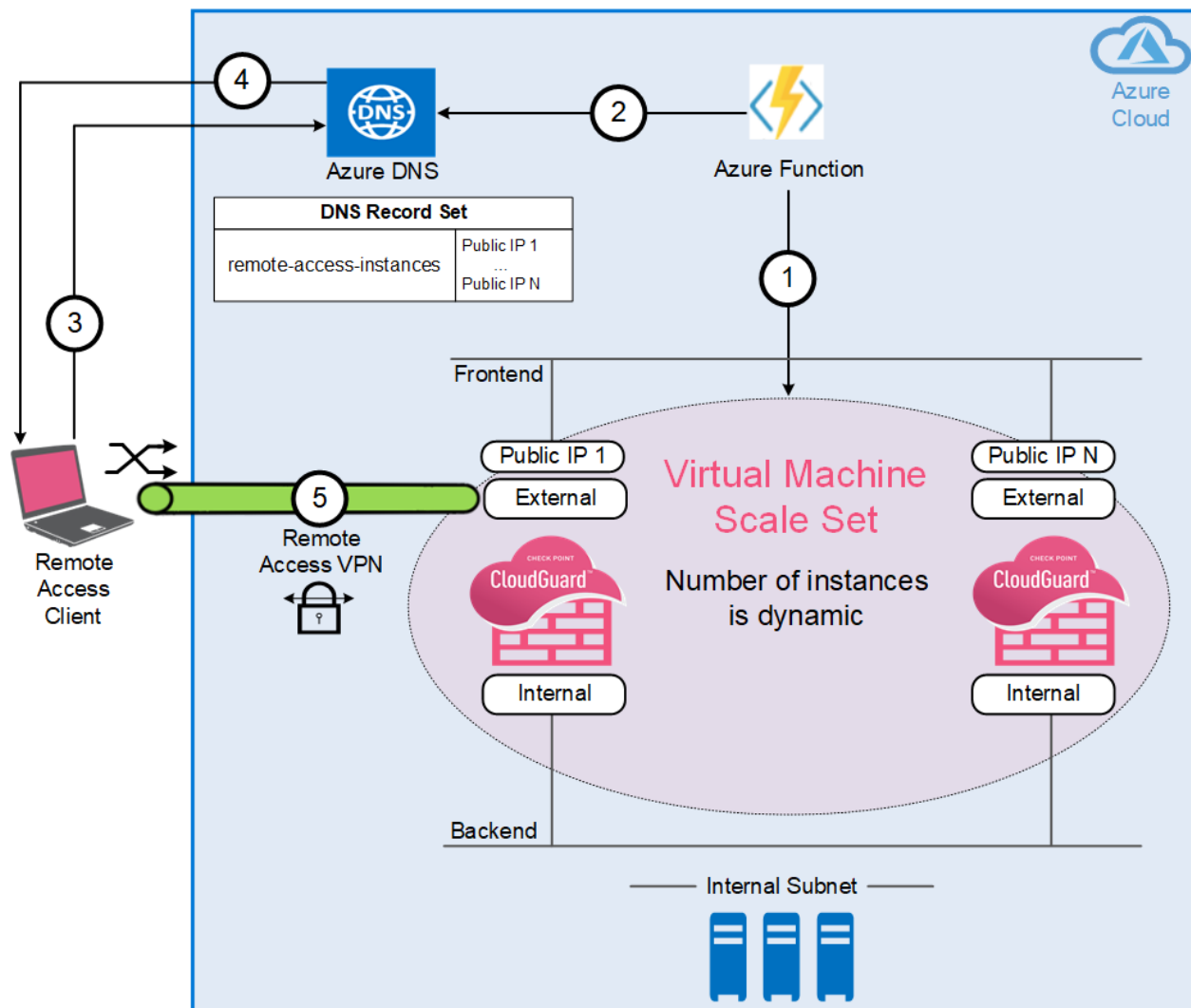
If the Remote Access VPN is enabled, during the configuration, these additional resources are deployed:

- **Function App (Azure function)**
- **System Assigned Managed Identity**
- Azure Function Application Insights
- Azure Function App Service Plan
- Azure Function Storage account

Network Diagram



Remote Access VPN Solution: High Level Architectural Diagram:



Action / Description	
1	Azure function gets Public IPs of VMSS instances whose provision process is finished.
2	Azure function creates, in case it does not exist, or updates a DNS Zone Record Set with the VMSS Instances' public IPs.
3	Remote Access VPN client runs a DNS query to resolve the current active IP addresses.
4	Azure DNS returns the current active IP addresses.
5	Client does a load-share mechanism on the resolved IP list and establishes Remote Access VPN connection with the appropriate VMSS instance. It then gets access to internal resources.

For Remote Access VPN limitations, see "[Known Limitations](#)" on page 27.

Remote Access VPN

- On each attempt to create a site or connect to the site, the client runs a DNS query to resolve the current active IP addresses and do a load-sharing mechanism on the resolved IP list.
- When the client initiates the connection, IKE negotiations take place with the configured Gateway on Azure. After the negotiations finish, a Remote Access tunnel is established.
- As part of the IKE negotiations, the Gateway assigns a special IP called *Office Mode* to the client. By this assignment, the Gateway can identify the Remote Access client and give it access to the internal resources - derived from the configured Policy in SmartConsole.

**** Only VPN Clients that you will find in this guide (page 23) support the described connection enhancement to VMSS CloudGuard Gateways.**

Configuration Steps

Step 1 Create an Azure AD and Service Principal

For a video instruction, click [here](#)

With the Azure AD and Service Principal, the Check Point Security Management Server monitors the creation and status of the VMSS, so it can finish the provision of these gateways.

From the Azure website, go to [Create an Azure Active Directory Application and Service Principal](#).

Use these parameters:

Field	Parameter
Name	Application_Name Example: <input type="text" value="check-point-autoprovision"/>
Application Type	Web-App / API
Sign-on URL	https://localhost/<Application_Name> Example: <input type="text" value="https://localhost/check-point-autoprovision"/>

After you create the application, write down these values, because you will use them in "[Step 3: Configure the Check Point Security Management Server](#)" on page 11:

- Application (client) id
- Client_Secret
- Directory ID
- Subscription ID

Note - We recommend that you set the key to **never expire**.

Step 2: Deploy the Azure App Service Domain and Assign the Azure AD Application

For a video instruction, click [here](#)

This step is required for Remote Access VPN configuration.

The App Service Domain (DNS Zone) is used to store the Record Set with the VMSS Instances' public IPs. Remote Access VPN clients run a DNS query to the Record Set FQDN to resolve the current active IP addresses and do a load-share mechanism on the resolved IP list.

Deploy the Azure App Service Domain <https://portal.azure.com/#create/Microsoft.Domain> from the Azure Portal

Notes:

Skip this step if you already have an existing Azure App Service Domain to use for the Remote Access solution.

To use an existing domain name registrar, it must be delegated to the Azure DNS Zone. For more information, see the [DNS Delegation Document](#)

For more information, see the [Microsoft Azure documentation](#).

Use these parameters:

Parameter	Description
Search for domain	The domain name that you want to buy and validate its availability.
Subscription	The Azure subscription where the App Service Domain is deployed.
Resource group	The Azure Resource Group where the App Service Domain is deployed.
Contact information	The Domain registration information.
Privacy protection	Accept terms and purchase.

Step 3: Configure the Check Point Security Management Server

For a video instruction, click [here](#)

Connect to the command line on the Security Management Server / Multi-Domain Security
Log in to the Expert mode.

1. Edit the file fwrl.conf

```
vi $FWDIR/conf/fwrl.conf
```

Add the following line ABOVE the "% SEGMENT DBLOAD" line:

```
NAME = conf/trac_client_1.ttm; DST = conf/trac_client_1.ttm;
```

Note: If this line is added in the wrong place, database installation would fail without an error message.

```
NAME = conf/rule_adtr.C; DST = conf/rule_adtr.C;
NAME = conf/trac_client_1.ttm; DST = conf/trac_client_1.ttm;
% SEGMENT DBLOAD
NAME = db, objects; FUNC = database_load; COMPRESS = minizip;
```

Save the Changes (wq!)

** For MDM follow the instructions in [sk55502](#).

2. Edit the trac_client_1.ttm file on the Management Server:
 - a. On the Multi-Domain Security Management Server, switch to the context of the involved Domain Management Server:

```
[Expert@HostName:0]# mdsenv <Name of Domain Management Server>
```

- b. Edit the trac_client_1.ttm file. Run:
 - i. vi \$FWDIR/conf/trac_client_1.ttm
 - ii. Set the automatic_mep_topology default value to false.

```
)
:automatic_mep_topology (
  :gateway (
    :map (
      :false (false)
      :true (true)
      :client_decide (client_decide)
    )
    :default (false)
  )
)
```

- iii. add this section to the file:

```

:enable_secondary_connect (
  :gateway (
    :map (
      :true (true)
      :false (false)
      :client_decide (client_decide)
    )
    :default (false)
  )
)

```

```

(
:enable_secondary_connect (
:gateway (
:map (
: true (true)
: false (false)
: client_decide (client_decide)
)
:default (false)
)
)
:trac_client_1 (
:neo_remember_user_password (
:gateway (endpoint_vpn_remember_user_password
:default (client_decide)
)
)
)

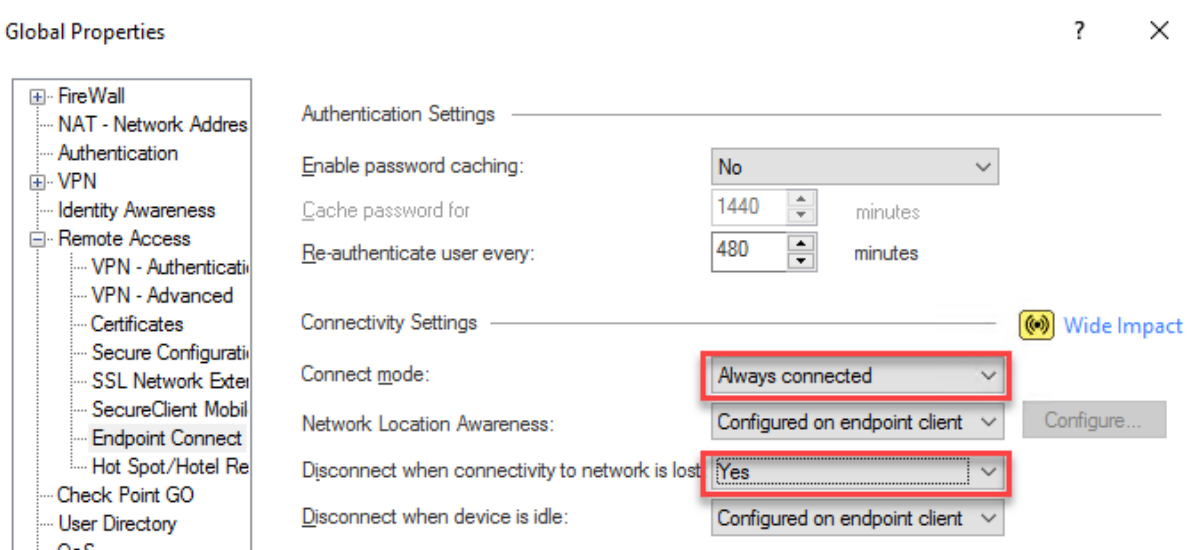
```

Note - If this section already exists, modify the "default" value to (false).

Save the changes (WQ!)

Do the bellow steps in SmartConsole

1. Open **Global Properties**.
2. Click the **Remote Access** tab.
3. Click **Endpoint Connect**.
4. Set the Connect Mode to **Always Connected**.
5. Set the **Disconnect** when network connectivity is lost to **Yes**.



6. Create a Network object to represent the entire external Gateway's address space:
 - a. Select the **Objects** menu > **New Network**.
 - b. Enter a descriptive name. For example, FrontEndNetwork.
 - c. From the left tree, click **General**.
 - d. Enter the applicable information.
 - e. Click **OK**.
7. In **Security Policies** > **Access Control**, , click **NAT** and add a Manual NAT rule to skip NAT for outbound traffic:
 - Original Source - Network Group object that represent the entire external Gateways address space
 - Original Destination - Any
 - Original Services - *Any
 - Translated Source - Original
 - Translated Destination - Original
 - Translated Services - Original
 - Install On - *Policy Targets

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destin...	Translated Services	Install On	Comments
1	FrontEndNetwork	* Any	* Any	= Original	= Original	= Original	* Policy Targets	

Automatic Generated Rules : Machine Static NAT (No Rules)

Add "Server Authentication" to the Extended Key Usage (EKU) of the GW IKE Certificate

1. Add an inbound security rule to the network security group to allow TCP access to port 18265 for the Management network interface.
2. Set up the ICA Management Tool, see [sk30501](#).
3. Access the ICA Management Tool go to this [link](#).
4. Click **Configure the CA**.
5. Below the **IKE Certificate extended key usage**, select **Server Authentication** > click **Apply**.
6. Disable the ICA management tool. On the Management Server, in Expert mode run:
`cpca_client set_mgmt_tool off`
7. Remove the security rule that allows TCP access to port 18265 for Management network interface the network security group.

Install The Latest CME and configure its service

1. Install the latest CME ([sk157492](#))
2. To check that the CME is installed run the command: `autoprov_cfg -v`

Note: If you get an unrecognized command error, open a new terminal window to the management and run the command again.

3. The instructions below contain information about configuring a VMSS environment in CME. For more information about CME configurations, see the [CME R80.10 and Above Administration Guide](#).

To configure the CME on the Security Management Server

Step	Description
1	Connect to the command line on the Security Management Server.
2	Log in to the Expert mode.
3	<p>Execute this command (see the explanation of parameters below):</p> <pre>autoprov_cfg init Azure -mn "<Management-Name>" -tn "<Configuration-Template-Name>" -otp "<SIC-key>" -ver <Version> -po "<Policy-Name>" -cn "<Controller-Name>" -sb "<Azure-Subscription>" -at "<Active-Directory-Tenant-ID>" -aci "<Client-ID>" -acs "<Client-Secret>"</pre> <p>add these parameters at the end (see the explanation of Remote Access parameters below):</p> <pre>-om "<Office-Mode-CIDR>" -ed "<Encryption-Domain-CIDR-List-separated-by-commas>" -dns "<Office-Mode-DNS-List-separated-by-commas>" (optional) -dns_suf "<Office-Mode-DNS-suffixes-separated-by-commas>" (Optional)</pre> <p>Example:</p> <pre>autoprov_cfg init Azure -mn "my-management" -tn "my-configuration-template" -otp "MySICkey123" -ver R80.10 -po "Standard" -cn "Azure-Production" -sb "98e34f37-ece4-4cdc-97dc-44a074f84aff" -at "7113cebb-911c-4122-aa5c-34db449380f7" -aci "82fb1445-f40e-46dc-9cd3-c065e14f132b" -acs "GafaerW8g_0369.Wu p60xV-06 . RlhMO " -om "10.0.1.0/24" -ed "172.168.1.0/24,172.168.2.0/24" -dns "10.0.2.4,10.0.2.4.5" -dns_suf "mydns1,mydns2"</pre>
4	<p>When this message shows, type yes and press Enter to apply the modifications:</p> <pre>Would you like to restart the autoprovision service now?</pre>

Step	Description
5	Confirm the configuration: <pre>[Expert@HostName:0]# service cme test</pre> Every controller in the configuration has to have unique credentials.
6	Follow the instructions in the <i>Enabling and Disabling Software Blades</i> section in CME R80.10 and Above Administration Guide .

Parameters:

Parameter	Description	Example
"<Management-Name>"	Select a descriptive name. When you deploy the Check Point VMSS with this name, the Check Point Security Management Server identifies and automatically provisions it.	"my-management"
"<Configuration-Template-Name>"	Configurations that automatically provision the Security Gateways in the VMSS are found in this template. When you deploy the Check Point VMSS with this template name, it references the relevant set of configurations to apply to it. Therefore, you can maintain multiple sets of configurations and associate them with different VMSS that are managed by the Security Management Server.	"my-configuration-template-for-x"
"<SIC-key>"	Select a random key that has at least 8 alphanumeric characters.	"MySICkey123"
<Version>	The Security Gateway version. One of these: <ul style="list-style-type: none"> R80.40 	R80.40
"<Policy-Name>"	The name of the policy to install. The name of this policy has to be the exact same name of the policy in SmartConsole. Note - This solution only supports R80.10 and Above. For R77.30, see sk115533 .	"Standard"

Parameter	Description	Example
"<Controller-Name>"	Select a name that represents the controller. The controller name includes configurations for your Azure environment, such as the subscription ID and application ID. You can maintain different controllers to automatically provision different Cloud environments, with the Security Management Server.	"Azure-Production"
"<Azure-Subscription>"	The Azure subscription ID that deploys the CloudGuard Security Gateways.	"98e34f37-ece4-4cdc-97dc-44a074f84aff"
"<Active-Directory-Tenant-ID>"	The Azure directory tenant ID.	"7113cebb-911c-4122-aa5c-34db449380f7"
"<Client-ID>"	The application ID.	"82fb1445-f40e-46dc-9cd3-c065e14f132b"
"<Client-Secret>"	The application key. Note - This value is not readable in the configuration.	

Remote Access VPN parameters

Parameter	Description	Example
"<Office-Mode-CIDR>"	<ul style="list-style-type: none"> ▪ This parameter is for Remote Access VPN configuration only. ▪ Office mode CIDR is used for Remote Access VPN. ▪ If Remote Access VPN is configured for multiple templates, then appropriate office mode addresses cannot collapse. 	"10.0.1.0/24"

Parameter	Description	Example
"<Encryption-Domain-CIDR-List-separated-by-commas>"	<ul style="list-style-type: none"> This parameter is for Remote Access VPN configuration only. This parameter is OPTIONAL. The client encryption domain networks is used for Remote Access VPN. 	"172.168.1.0/24,172.168.2.0/24"
"<Office-Mode-DNS-List-separated-by-commas>"	<ul style="list-style-type: none"> This parameter is OPTIONAL. Office mode DNS addresses used for a specific Remote Access VPN configuration. A maximum of three Office mode DNS addresses can be configured. 	"10.0.2.4,10.0.2.5"
"<Office-Mode-DNS-suffixes-separated-by-commas>"	<ul style="list-style-type: none"> This parameter is OPTIONAL. To configure, you need "<Office-Mode-DNS-List-separated-by-commas>". Office mode DNS suffixes used for a specific Remote Access VPN configuration. 	"mydns1,mydns2"

Important:

The exact values that you select, must be typed exactly when you deploy the VMSS Azure Template. Make sure to write them down and enter them correctly. Otherwise, the components cannot communicate with each other.

1. CPM objects are created automatically during CME initialization:

- Network object that represents the "<Office-Mode-CIDR>" called
"om_net_pool_<Configuration-Template-Name>"
- Group object that represents the Encryption Domain called:

"enc_dom_net_pool_<Configuration-Template-Name>"

Note - This object exists only if "< Encryption-Domain-CIDR-List-separated-by-commas>" was configured, or CME did provision at least one Scale Set instance.

- Host objects that represent each configured Office Mode DNS called:

"om_dns_host_member_[1-3]_<Configuration-Template-Name>"

Note - This object exists only if "<Office-Mode-DNS-List-separated-by-commas>" was configured.

There is an option to modify the Office Mode subnet and the Encryption Domain with these steps:

- a. Open SmartConsole and connect to the Management Server.
- b. To update the Office Mode subnet object, locate and edit the Office Mode object.
- c. To update the Encryption Domain, locate and edit the Encryption Domain object.
- d. Publish the SmartConsole session.
- e. Install policy on all Scale Set instances.

Note - The created objects are not automatically deleted by CME.

2. If a Multi-Domain Server is used, make sure that the Domain Server is configured as required in CME. Do this before the Remote Access VPN configuration is added.

Step 4: Deploy the Check Point VMSS and Assign the Azure AD Application

For a video instruction, click [here](#)

Deploy the [CloudGuard IaaS - Firewall and Threat Prevention](#) from the Azure Marketplace.

- **Use these parameters in the Basic section:**

Parameter	Description
Gateway scale set name	The name of the VMSS resource group.
Credentials	The public key or username and password for SSH connections to the CloudGuard IaaS Gateway.
Subscription	The Azure subscription, where the VMSS is deployed.
Resource group	The Azure Resource Group, where the VMSS is deployed. Important - The Resource Group must be empty.
Location	The location - where the VMSS is deployed.

- **Use these parameters in the Check Point VMSS settings section:**

Parameter	Description
Are you upgrading your CloudGuard VMSS solution?	Defines whether this a new deployment, or purpose of this deployment is to upgrade an existing VMSS deployment. If this is an upgrade of the CloudGuard VMSS solution, select Yes .
Initial number of Security Gateways	The minimum number of CloudGuard IaaS Gateways instances in the VMSS. We recommend a minimum of two.
Maximum number of Security Gateways	The maximum number of CloudGuard IaaS Gateways instances in the VMSS.
Management name	The name of the Security Management Server. Example: <input data-bbox="703 808 1460 864" type="text" value="my-management"/> See, " Configuring the CME (Cloud Management Extension) on the Security Management Server " on page 13
Configuration template name	The name of the configuration template from the CME service. Example: <input data-bbox="703 1115 1460 1171" type="text" value="my-configuration-template"/>
Administrator email address	The email address of the Administrator responsible for scaling operations, such as the launch of a new gateway, or a gateway termination.
Load Balancer deployment	Defines which Load Balancer to deploy: <ul style="list-style-type: none"> • Standard (External & Internal inspection). • External only (Inbound inspection only). • Internal only (Outbound & East-West inspection only). For outbound inspection, it is mandatory to deploy an External Load Balancer and, or instance level public IP addresses.
Check Point CloudGuard External Load Balancer session persistence	The load balance distribution method for the External Load Balancer - Inbound. See, Configure the distribution mode for Azure Load Balancer .

Parameter	Description
Check Point CloudGuard Internal Load Balancer session persistence	<p>The load balance distribution method for the Internal Load Balancer - Outbound and East-West.</p> <p>See, Configure the distribution mode for Azure Load Balancer.</p>
Deploy the VMSS with instance level public IP address	<p>If you select yes, each VMSS instance gets its own public IP address.</p> <p>The Security Management Server can use those IP addresses to manage from the external VNET.</p> <p>Default value: no.</p> <p>Important - The value you configure is irreversible.</p> <p>When the Remote Access VPN is used, you must manage VMSS with public IPs.</p>
Management interface and IP address	<p>Select which IP address to use as the management interface for the VMSS:</p> <ul style="list-style-type: none"> Backend NIC's private IP address. Frontend NIC's public IP address - only available if you deploy an Instance Level Public IP (ILPIP) address. Frontend NIC's private IP address. <p>Private:</p> <p>Manage the Gateway VMSS with the private IP address of the instance. The Security Management Server must have access to the private IP addresses. For example, to be in the same/peered VNET.</p> <p>In case you use the frontend NIC, you must add a corresponding rule in the Frontend Route Table: <i>Destination & Next Hop: <The private IP address of the Security Management Server></i>.</p> <p>Public:</p> <p>Manage the Gateway VMSS with the public IP address of the instance.</p> <p>Note:</p> <p>Support for private addresses is available with Add-On version 419 and above, and template version 20200303 and above.</p>

Parameter	Description
Number of Availability Zones to use	<p>Defines the Azure Availability Zones for your VMSS:</p> <ul style="list-style-type: none"> • None - Do not use Azure Availability Zones. • 1 - Use Azure zonal redundancy. • 2 - Use Azure two-zones redundancy (zones [1, 2]) • 3 - Use Azure three-zones redundancy (zones [1, 2, 3]) <p>Notes:</p> <ul style="list-style-type: none"> • Only available if you deploy in a supported Azure location. • Support for Azure Availability Zones is available with template version 20200303 and above.
Remote Access VPN settings	<p>If you select yes, the Remote Access VPN required Azure resources, Azure function, and System Assigned Managed Identity, are deployed and configured.</p> <p>Note - Select yes only in case Remote Access VPN functionality is used.</p>
DNS Resource Zone ID	<p>Resource Id is the unique, permanent, identifier assigned to each Azure resource. The DNS Zone Resource id its related Properties tab.</p>
DNS Record Set Name	<p>DNS Record that includes a maximum of 20 public IPs of VMSS instances. If a current Record Set is used, all its records are replaced with the VMSS instances' public IPs.</p>

▪ **Use these parameters in the Network settings section:**

Parameter	Description
Network setting	<p>A pre-existing Virtual Network and its subnets, or the name of a new Virtual Network and subnets, where the VMSS is deployed.</p> <p>Note:</p> <p>When you use a pre-existing subnet:</p> <ul style="list-style-type: none"> • Make sure no other Virtual Machines are deployed in those subnets • Make sure to correctly define user defined routes (UDR) for each subnet (see the section).

1. Assign the Azure Active Directory application as described in Step 1: "[Step 1 Create an Azure AD and Service Principal](#)" on page 8. Add a minimum role of **Reader** to both the VMSS and the VNET. See [Assign application to role](#).
2. If Remote Access VPN is used, do these steps:

- a. Assign the Azure AD application as described in Step 1 ("Step 1: Create an Azure AD and Service Principal" on page 8). Add a minimum role of **Reader** to the VNET and the role of **Contributor** to the VMSS.
- b. Assign System Assigned Managed Identity application is created as part of the VMSS deployment. Add a minimum role of **Contributor** to the Resource Group of the App Service DNS (DNS Zone). The name of the System Assigned Managed Identity is equal to the VMSS Resource Group one.

For more about Managed identities, see the [Azure documentation overview](#).

Notes:

- Newly provisioned Security Gateways automatically receive the latest published Security Policy. You have to install the policy on the existing Security Gateways to update their Security Policy.
- Auto Scaling Security Gateway objects are automatically created and deleted according to the current environment. Therefore, we do not recommend that you use specified objects in rules. We also do not recommend that you manually edit those objects.
- In case of Scale-Out event, the latest released Check Point image is used to deploy the new Virtual Machine.
- As part of Remote Access VPN deployment, the azure function (also called "Function App") is deployed. The azure function is triggered every two minute. Its purpose is to get VMSS provisioned instances and add their public IPs to the DNS Zone Record Set.

For more information:

- CloudGuard for Azure Latest Updates - see [sk132192](#)
- Blink - Gaia Fast Deployment - see [sk120193](#)
- By default, every Check Point Security Gateway and Security Management Server's WebUI is accessible from the internet, see <http://<virtual-machine-public-ip>>. Access restrictions to the WebUI is possible. You need to configure a Network Security Group, or configure the Check Point Gateway and Management Server settings.

Step 5: Deploy the Azure Function Code

For a video instruction, click [here](#)

Do this step to deploy the Azure Function code in the Azure Function Storage Account. The Azure Function

Responsibilities include: monitor the VMSS instances and update the DNS Record Set accordingly

Step	Instructions
1	Download the Azure Function code from this link .
2	From the Azure portal, navigate to the VMSS Resource Group.

Step	Instructions
3	<p>Click on the Function App storage account. Note - The Azure Function App storage account name always starts with the "azurefunction" string.</p>
4	<p>In the storage account resource, click Containers > azure-function. Azure documentation says this: "When using Blob storage, you should use a private container with a Shared Access Signature (SAS) to enable the Functions runtime to access to the package". For more information, see the Azure Function Documentation.</p>
5	<p>Upload the zip archive with Azure function code to the azure-function container.</p>
6	<p>Open the zip archive and navigate to the Generate SAS tab.</p>
7	<p>Change the SAS token expiry date/time > click Generate SAS token and URL. Note - Make sure that the SAS token expiry date and time is configured correctly. After</p> <ul style="list-style-type: none"> the SAS token expires, the Azure Function stops its executions
8	<p>Select and copy Blob SAS URL. Note - The Blob SAS URL for the Azure Function code zip archive is accessible over the Internet.</p>
9	<p>Navigate back to the VMSS Resource Group > click the App Service (Function App) resource. Note -The Azure Function App storage account name is always equal to the VMSS Resource Group name..</p>
10	<p>In the Function App resource, select Configuration > Application settings > click WEBSITE_RUN_FROM_PACKAGE.</p>
11	<p>Paste the SAS URL to the Value field > Click OK.</p>
12	<p>In the Configuration view, Click Save.</p>

Step 6: Configure and Deploy the Remote Access VPN Client

For a video instruction, click [here](#)

Download the [Endpoint Security VPN standalone](#) or the [Endpoint Security Managed client package](#).

For information on the client deployment and distribution options, see "Setting Up Remote Access Clients" in [R80.10 and Higher Remote Access VPN Administration Guide](#) RA Client Admin guide for Windows (standalone client) or the "Deploying Endpoint Security Clients in this Guide" in the [R80.40 Endpoint Security Server Administration Guide](#) (for the Endpoint Security Managed client)

When you create the VPN site on the client, it is important to configure the site's DNS name in the **Server address or name**. This is for the client to resolve the IP list and do a load share on the resolved IP list.



Best Practice - While the client moves between the site's Gateway (scale in and out events), it is recommended to use the CAPI certificate for the user authentication method.

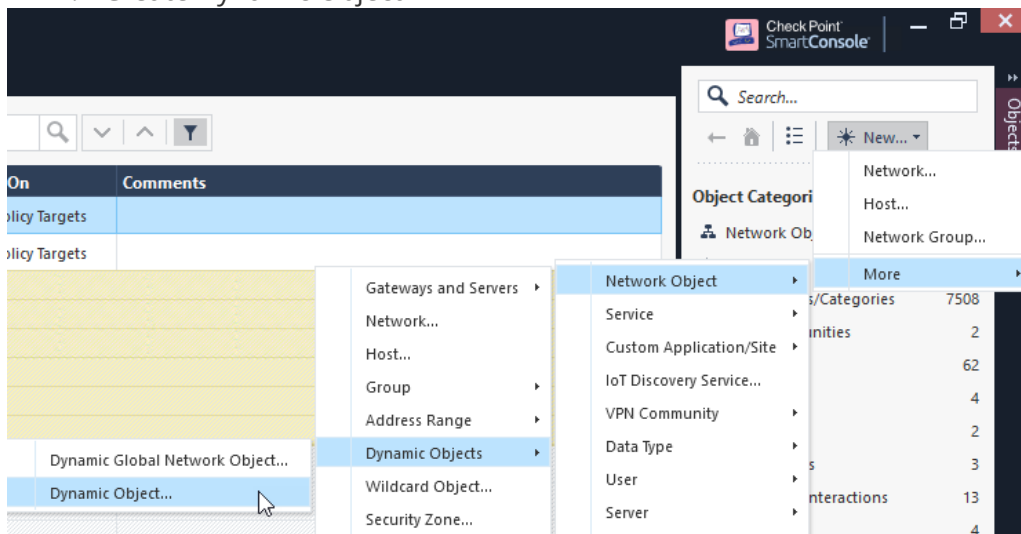
Step 7: Create a Source NAT rule for Office mode ip address range network (for route back)

For a video instruction, click [here](#)

Add a Manual NAT rule to hide the ip office mode ip addresses (VPN Clients office mode ip) behind the gateway internal interface ip address.

As the CloudGuard gateway scale in and out dynamically and their ip address assign automatically. We will create first a Dynamic object that will represent the internal ip address of the Cloudguard.

1. Create Dynamic Object



2. Give the object the name: LocalGatewayInternal
3. On the Azure-AutoScale-1 policy, navigate to NAT Policy.
4. Create new NAT rule in the top of the policy.
5. Original Source - The office mode network object that have been created by the CME.
6. Original Destination - The Spokes networks group
7. Original Services - *Any
8. Translated Source - The Dynamic Object: LocalGatewayInternal
9. Translated Destination - Original
10. Translated Services - Original
11. Install On - *Policy Targets
12. Push Policy.

Troubleshooting

- See the Azure portal to check the health probe logs and make sure that the CloudGuard Security Gateways respond to [health probes](#).

Note - The health probes arrive from a special IP address 168.63.129.16. See the Microsoft blog post on '[What is the IP address](#)'.

Remote Access VPN

Remote Access VPN configuration adds to the regular VMSS deployment the Azure function and App Service Domain (DNS Zone) resources. This description shows how to monitor the health of the resources.

Azure function (Function App):

1. From the Azure portal, navigate to the **Azure Function App** resource.
2. Select **Function App** with the VMSS resource group name.
3. Navigate to the **Functions** tab > click the function's name.
4. Navigate to the **Monitor** tab:
 - a. Make sure the function execution status is successful.
 - b. To see the full log, click on a function execution date.

DNS Zone:

1. From the Azure portal navigate, to the **DNS Zones resource**.
2. Navigate to the DNS Zone. Use the name defined in the VMSS deployment.
3. Make sure the DNS Zone Record Set includes the VMSS Instances' public IPs.

For Gateway issues, refer to the [Solution Center](#).

Known Limitations

- Refer to [sk109141](#) for more information on supported Jumbo Hotfixes.
- Refer to [sk157492](#) for more information about CME limitations.
- To manage R80.20 VMSS with R80.10 Management Server, you must install R80.10 Jumbo Hotfix Accumulator (R80.10_jumbo_hf) - *Take 169* and above.
- IPv6 is not supported.
- Only Azure Resource Manager (ARM) deployments are supported.

Deployment in the Azure classic environment is not supported.

- Azure Load Balancers have limits. There is a limit on the number of front-end IP addresses it supports.

See Microsoft documentation on [Azure Networking Limits](#).

- East-West inspection between peered VNets is supported only for RFC 1918 private networks (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).
- Anti-Spoofing on the internal NIC of the VMSS instances (`eth1`) is disabled by default and must not be enabled.
- If the Endpoint Policy Management Software Blade is enabled on the Security Management Server, then the Autoprovision feature is not supported.
- Azure DNS does not replace the client's DNS Servers. It can be used in addition to public and ISP DNS servers. For more information, see [Microsoft Azure DNS documentation](#).
- Remote Access Secondary Connect is not supported.
- Policy Server (Desktop Policy) is not supported.
- Remote Access client Back connections are not supported.
- For Endpoint Security managed clients, Enforcing Firewall policy from the SmartDashboard is not supported.
- For Endpoint Security managed clients, configuration of SCV checks from the Gateway is not supported.

- Hub Mode (Route-All-Traffic) is not supported.
- Editing Login Options and Legacy Authentication is not supported.
- Automatic MEP Topology is not supported.
- Machine Authentication is not supported.
- For Endpoint Security VPN, SecuRemote flavor is not supported.
- Editing office mode configuration is not supported. This includes Office Mode IP Address per User (`IPAssignment.conf`).
- Editing Link Selection configurations is not supported.
- Perform Anti-Spoofing on Office Mode addresses is not supported.
- Connection enhancements for gateways with multiple external interfaces (also known as "magic button") are not supported.
- Site to Site VPN is not supported.
- **Instance Level Public IP (ILPIP) address**

Because of Microsoft Azure design, if you deploy a Check Point Security Gateway with an ILPIP address to manage the VMSS by its public IP addresses:

1. Each instance is configured in Check Point SmartConsole with the original (first) ILPIP address.
2. If the deployed Check Point Security Gateway is restarted, the ILPIP address could be released by Microsoft Azure and a new IP address is dynamically allocated.

In such case:

- The Check Point Security Gateway still functions.
- However, the Check Point Management Server is no longer able to communicate with the Check Point Security Gateway (this affects policy installation, receiving logs, monitoring).

These two options are available:

- Delete the instance in Azure portal and let Azure bring up a new one (which is then automatically recognized by the Check Point Management Server)
- Manually reset the SIC:
 - a. Reset the SIC in SmartConsole and on the Check Point Security Gateway instance.
 - b. In SmartConsole, manually change the IP address of Check Point Security Gateway object to the new dynamically assigned IP address.
 - c. In SmartConsole, manually initialize the SIC.

Check Point Copyright Notice

© 2020 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](#) for a list of our trademarks.

Refer to the [Third Party copyright notices](#) for a list of relevant copyrights and third-party licenses.