CloudGuard Deployment in Microsoft Azure

Summary:

This whitepaper walks through the creation of an Azure environment with a Check Point CloudGuard firewall protecting a Web Server. The Azure environment consists of a VNet with three subnets: Frontend, Backend and Web. The CloudGuard firewall will have a NIC in the Frontend and Backend subnets and the Web Server will be deployed in the Web subnet. A Check Point R80.20 Security Management Server will be deployed in the Frontend subnet and integrated with the CloudGuard Controller.

Prerequisites:

- You will need a Microsoft Azure account with a valid subscription
- Basic understanding of the following Azure Services:
  - Azure Virtual Networks: An Azure Virtual Network (VNet) is a representation of your network in the cloud. It is a logical isolation of the Azure cloud dedicated to your resources.
  - User Defined Routes: AKA Azure Route Tables, allow you to create network routes so that your Check Point CloudGuard firewalls can handle traffic between all subnets and destined for outside the VNet.
  - Virtual Machines: Provide flexibility of virtualization for a wide range of computing solutions.
- Basic admin experience with SmartConsole
  - How to create/modify objects
  - How to create/modify rules in a policy
  - How to publish sessions and install policy
  - How to view logs

Additional Resources:

- Recorded demonstration of this deployment: https://www.youtube.com/watch?v=HX3mG-hjSDo
- Check Point Secure Knowledge Article sk109360 – Check Point Reference Architecture for Microsoft Azure
- Check Point Secure Knowledge Article sk132192 – CloudGuard for Azure Latest updates
Deployment Steps:

1. How to create a Virtual Network with a Frontend subnet
   a. Navigate to Virtual Networks and click Create
   b. Name: myVNET
   c. Address space: 10.0.0.0/16
   d. Choose your subscription
   e. Create new Resource Group: myVNET-RG
   f. Location: West US
   g. Subnet:
      i. Name: Frontend
      ii. Address range: 10.0.0.0/24
   h. Leave the rest as default and click Create

2. Add two more subnets to the Virtual Network
   a. Click on myVNET
   b. Navigate to Subnets and click on new Subnet
   c. Name: Backend
   d. Address range: 10.0.1.0/24
   e. No Network Security Group
   f. No Route tables
   g. Click OK
h. Click on **new Subnet**

i. **Name**: Web

j. **Address range**: 10.0.2.0/24

k. **No Network Security Group**

l. **No Route tables** (We will create this at a later time)

m. Click **OK**
3. How to deploy the R80.20 Management Server
   a. Search the Marketplace for Check Point
   b. Select Check Point Security Management and click **Create**
   c. Server Name: CPmanagement
   d. Authentication type: Password
   e. Choose Subscription
   f. Create Resource Group: CPmanagement-RG
   g. Location: West US
   h. Click **OK**
   i. Check Point CloudGuard version: R80.20
   j. License type: Bring Your Own License
   k. Virtual machine size: 1x Standard D3 v2
   l. Allowed GUI clients 0.0.0.0/0
   m. Allow download from/upload to Check Point
n. Click **OK**

o. Virtual Network: myVNET

p. Subnet: Frontend

q. Once validation passes click **Create**
4. How to deploy the CloudGuard firewall
   a. Search Marketplace for Check Point
   b. Select Check Point CloudGuard IaaS Single Gateway and click Create
   c. VM Name: CPgateway
   d. Authentication Type: Password
   e. Choose Subscription
   f. Create Resource Group: CPgateway-RG
   g. Select Location and click OK
   
   ![Create Check Point CloudGuard Gateway](image)
   
   h. Check Point CloudGuard Version: R80.10
   i. License Type: Bring Your Own License (Check Point gives default 15 day evaluation period)
   j. Virtual Machine Size: 1x Standard D3 v2
   k. Installation Type: Gateway only
   l. SIC key – Vpn123456789
   m. Allow download from/upload to Check Point
   n. Click OK
o. Virtual Network: myVNET
p. Frontend subnet: Frontend
q. Backend subnet: Backend
r. Click OK

s. Once validation passes click Create
5. Access Security Management Server Web UI to download SmartConsole
   a. Use browser to navigate to: https://YourMgmtPublicIP
   b. Click Download SmartConsole

6. How to create the gateway object in SmartConsole
   a. Open R80.20 SmartConsole using credentials defined during creation and SMS Public IP

   ![SmartConsole Login](image)

   b. Create a new gateway object
      i. Name: cpgateway
      ii. Platform: CloudGuard IaaS
      iii. Gateway IP address: Static - Use the gateway’s frontend private IP (10.0.0.5)
      iv. Click Next
      v. Initialize SIC
      vi. Click Next
      vii. Disable Anti-Spoofing on both NICs
          i. Go to Network Management and double click `eth0` and `eth1`
          ii. Modify Topology and disable Anti-Spoofing on both interfaces. Anti-Spoofing is already done by Azure.
c. Create a permissive policy by changing Cleanup rule to:
   i. Action: Accept
   ii. Track: Log

d. Install only Access Control policy

7. Access firewall Web UI to create a static route
   a. Use browser to navigate to: https://YourGWPublicIP
   b. Create route on firewall to route traffic destined for the Web Subnet through the internal firewall interface. This is required because the firewall is not directly connected to the Web Subnet
      i. Navigate to IPv4 Static Routes
      ii. Click Add
         i. Destination: Web Subnet address space – 10.0.2.0
         ii. Subnet mask: 255.255.255.0
      iii. Add Gateway IP
         i. Using first address of the Backend subnet as it represents the Azure router – 10.0.1.1

![Add Destination Route](image)

8. How to deploy the Web Server
   a. Search the Marketplace for Nginx Bitnami
      i. Select NGINX Open Source Certified by Bitnami
      ii. Choose Subscription
      iii. Resource Group: myVNET-RG
      iv. Virtual machine name: myWeb
      v. Region: West US
      vi. Authentication type: Password
vii. Click **Next : Disks** and leave settings as default
viii. Virtual network: myVNET
ix. Subnet: Web
x. Public IP: None
xi. Network Security Group: None

b. Click **Review + Create**
c. Once validation passes click **Create**
9. How to create the User Defined Routes:
   a. Navigate to Route Tables
   b. Click **Create route table**
   c. Name: myVNETroutes
   d. Choose Subscription
   e. Resource group: myVNET-RG
   f. Location: West US
   g. Click **Create**
   h. Once created, Navigate to Routes:
      i. Click **Add**
         i. Route name: Intra_VNET
         ii. Address prefix: 10.0.0.0/16
         iii. Next hop type: Virtual Appliance
         iv. Next hop address: Internal NIC of the firewall (10.0.1.4)
         v. Click **OK**
   j. Click **Add**
      i. DefaultGW
      ii. Address prefix: 0.0.0.0/0
      iii. Next hop type: Virtual Appliance
      iv. Next hop address: Internal NIC of the firewall (10.0.1.4)
      v. Click **OK**
   k. Navigate to Subnets
      i. Click **Associate**
      ii. Virtual Network: myVNET
      iii. Subnet: Web
      iv. Click **OK**

10. Defining Networks that sit behind internal NIC of firewall
    a. Edit cpgateway object
    b. Navigate to Network Management
       i. Modify Topology and Select Override
          i. Leads to Specific Networks
          ii. Create new address range object
             i. Name: Internal_Subnets
             ii. First IP Address: 10.0.1.1
             iii. Last IP Address: 10.0.2.255
11. Update Access Control Policy
   a. New rule:
      i. Name: Traffic to web server
      ii. Destination: cpgateway object
      iii. Service: http & https
      iv. Action: Accept
      v. Track: Log
   b. New rule below this
      i. Name: SSH to all
      ii. Service: ssh
      iii. Action: Accept
      iv. Track: Log
   c. New NAT rule
      i. Original Source: Any
      ii. Original Destination: cpgateway object
      iii. Original Services: http
      iv. Translated Source: Original
      v. Translated Destination: Create host object called WebServer with IP address of the Web server 10.0.2.4 (depends)
      vi. Translated Services: Original
   d. Install Access Control policy
12. Use a browser to navigate to the Public IP address of the firewall. Filter for http traffic in SmartConsole to see what is happening.
13. How to integrate the CloudGuard Controller
   a. Activate CloudGuard Controller on Management Server
      i. Use putty to ssh to Management Server
      ii. Type `cloudguard on` in expert mode

   b. Go to Azure Portal to create the authentication method which the SMS will use to access Azure environment
   c. Navigate to Azure Active Directory
      i. Navigate to Properties and Copy the directory ID
      ii. Navigate to App registrations
          i. Click New application registration
          ii. Name: CloudGuard-controller
          iii. Application type: Web app / API
iv. Sign-on URL: https://localhost/CloudGuard-controller
v. Click Create
iii. Copy Application ID

![Image]

iv. Click Settings
i. Navigate to Keys
   i. Description: CloudGuard
   ii. Expires: Never
   iii. Click Save
   iv. Copy Value

d. Now choose Resource Group or Subscription that SMS will have access to:
   i. Navigate to myVNET-RG
   ii. Select IAM
      i. Click Add
         i. Role: Contributor role
         ii. Assign access to: Azure AD user, group or service principal
         iii. Select CloudGuard-controller
         iv. Click Save

e. How to create the new datacenter object
   i. New object -> More -> Server -> Datacenter -> Microsoft Azure
      i. Name: Azure-Controller
      ii. Input Application ID
      iii. Input Secret key
      iv. Input Directory ID
   ii. Click Test Connection
      i. Connected means that Azure native objects can be used in policy

f. Publish session
14. We can now use Azure native objects in the policy
   a. Navigate to Access Control policy
   b. Click the + in Source or Destination of any rule
   c. Click Import
   d. Hover over Data Centers
   e. Click Azure-controller