

WELCOME TO THE FUTURE OF CYBER SECURITY

Deploying CloudGuard with Azure Application Gateway WAF

Chris Beckett chrisbe@checkpoint.com 7th November 2018

Contents

Deploying CloudGuard with Azure Application Gateway WAF	1
Introduction	2
Deployment Steps	2
Adding a backend pool	5
Upgrading the VMSS	6
Verifying backend health	7
Configuring Backend HTTP Settings	7
Create new TCP service in SmartConsole	8
Configuring Access Control and NAT Rules	8
Testing the connection	9
Troubleshooting	9
Revision History	9

Introduction

Check Point CloudGuard IaaS is deployed from the Azure Marketplace using a supplied ARM template that scripts the installation and configuration of Azure load balancers and Virtual Machine Scale Sets (VMSS).

As CloudGuard is not strictly a Web Application Firewall (WAF) but has WAF like capabilities, sometimes a WAF is required to complete any missing functionality and/or for design compliance, depending on the deployment scenario.

In order to add a WAF to a CloudGuard secured environment, the native Azure WAF can be deployed and used by deploying an Application Gateway instead of the external load balancer which is created by the Marketplace ARM template. This provides load balancing facilities as well as WAF functionality.

A diagram is shown below of a sample environment protected by the Azure Application Gateway, illustrating the change of external perimeter device from Azure load balancer to Azure Application Gateway.

The benefits of this solution include WAF capabilities, auto scaling (provided by the VMSS) and connection draining during scale in operations.



Deployment Steps

As a pre-requisite, it is assumed that the Check Point Management server is present and has the ability to manage the Azure environment. The CloudGuard scale set Marketplace solution should also be deployed as per the diagram below. To keep the deployment simple, it is recommended to choose the "Internal Only" load balancer deployment.

The purpose of this is to ensure an external load balancer is not created that is not used and may incur further charges. For testing purposes, place a web server into the web subnet as shown in the diagram below, in this example we will use Nginx running on Linux.

Once the VMSS has been created with the internal load balancer, the next step is to create the Azure Application Gateway.

Creating the Azure Application Gateway

The Application Gateway is created from the Azure Portal by clicking the top left "Create a resource" button. In step 1 of the wizard, give the Application Gateway a name, choose the appropriate tier (WAF), instance count (minimum of 2 is recommended), SKU size (Medium is recommended for testing purposes), subscription, resource group and location.

1 Basics Configure basic settings Name wafv2 Tier Capacity type Autoscale Manual Minimum scale units 2 Subscription Visual Studio Professional Resource group (New) rg-wafv2 Create new Location North Europe Availability zone None Vour virtual network and public IP alores smuth to in the same location as your spreave, if you plan on using existing resources, pusite that you select the correct 	 Basics Configure basic settings 2 Settings Configure application gateway 3 Summary Review and create 4 Minimum scale units 2 Capacity type Autoscale Manual Minimum scale units Minimum scale units 2 Capacity type Autoscale Manual Minimum scale units Minimum	 Basics Configure basic setting: 2 Settings Configure application gateway 3 Summary Review and create Minimum scale units Autoscale Manual Minimum scale units 2 < Subscription Visual Studio Professional Resource group (New) rg-wafv2 Create new Location North Europe Availability zone None Vour virtual network and public IP address must be in the same plan on using existing resources, ensure that you select the correct location. 	 Basics Configure basic settings 2 Settings Configure application gateway 3 Summary Review and create Niminum scale units Autoscale Manual Minimum scale units Subscription Visual Studio Professional Resource group (New) rg-wafv2 Create new Location North Europe Availability zone None Iori Manual Our virtual network and public IP algoes must be in the same floation argoing existing resources ensure that you select the correct 	1 Basics 2 Settings Configure basic settings * There WaFV2 Configure application gateway 3 Summary Review and create * </th <th>Create application gateway</th> <th>×</th> <th>Basics</th>	Create application gateway	×	Basics
Users ✓ Configure basic settings ✓ 2 Settings ✓ Configure application gateway ✓ 3 Summary ✓ Review and create ✓ ✓ • Tier WaFv2 ✓ • Subscription ✓ Visual Studio Professional ✓ • Resource group ✓ (New) rg-wafv2 ✓ • Location ✓ None ✓ Out wind network and public IP algess must be in the same location as your greave, If you plan on using existing resources, group election as your greave, If you plan on using existing resources, group election as your greave, If you plan on using existing resources, group election as your greave, If you plan on using existing resources, group election as your greave, If you plan on using existing resources, group election as your greave, If you plan on using existing resources, group election as your greave, If you plan on using existing resources, group election as your greave, If you plan on using existing resources, group election as your greave, If you plan on using existing resources, group election as your greave, If you plan on using existing resources, group election as your greave, If you plan on using existing resources, group election as your greave, If you plan on using existing resources, group election as your greave, If you plan on using existing resources, group electing existing resources, group election electing existing resource	Users Configure basic settings • Tier 2 Settings Configure application gateway • Tier 3 Summary Review and create • Manual • Minimum scale units • Subscription • Subscription Visual Studio Professional • Resource group • Netw rg-wafc2 • North Europe Availability zone • Nore Nore	Configure basic settings 2 Settings Configure application gateway 3 Summary Review and create Summary Review and create Manual Minimum scale units 2 2 Subscription Visual Studio Professional Visual Studio Professional North Europe Availability zone None	Lossis ✓ Configure basic settings ✓ 2 Settings ✓ Configure application gateway ✓ 3 Summary ✓ Review and create ✓ ✓ ✓ Minimum scale units ✓ ✓ Subscription ✓ ✓ Visual Studio Professional ✓ ✓ North Europe ✓ Availability zone ✓ ✓ None ✓ ✓	Loss ✓ Configure basic settings 2 Settings Configure application gateway 3 Summary Review and create Summary Visual Studio Professional • Resource group North Europe ✓ Vailability zone Nore	Parier		* Name
Settings Configure application gateway Summary Review and create North Europe ✓ Create mw Location North Europe ✓ Availability zone Nore ✓ Your virtual network and public IP address must be in the same location as your gateway.ff you plan on using existing resources, more weak and the same Nore ✓ Your virtual network and public IP address must be in the same location as your gateway.ff you plan on using existing resources, and the same location as your gateway.ff you plan on using existing resources, and the same location as your gateway.ff you plan on using existing resources, and the same location as your gateway.ff you plan on using existing resources, and the same location as your gateway.ff you plan on using existing resources, and the same location as your gateway.ff you plan on using existing resources, and the same location as your yealerthe correct	2 Settings Configure application gateway 3 Summary Review and create • Minimum scale units 2 • Subscription Visual Studio Professional • Resource group (New) rg-wafv2 • Create new • Location North Europe • Availability zone None	2 Settings Configure application gateway 3 Summary Review and create • Tier WAF V2 Capacity type Autoscale Annual • Minimum scale units 2 • Subscription Visual Studio Professional • Resource group (New) rg-wafv2 • Create new • Location North Europe Availability zone None Visual Attivation as your gateway, if you plan on using existing resources, ensure that you select the correct location	2 Settings Configure application gateway 3 Summary Review and create * Image: Configure application gateway 3 Summary Review and create * Minimum scale units 2 • * Subscription Visual Studio Professional • • Resource group (New) rg-wafv2 • • Location North Europe • • Availability zone None •	2 Settings Configure application gateway 3 Summary Review and create • Minimum scale units 2 • Subscription Visual Studio Professional • Resource group (New) rg-wafv2 • Create new • Location North Europe • Variability zone None	Configure basic settings		wafv2 🗸
2 Settings Configure application gateway 3 Summary Review and create * Minimum scale units 2 ✓ • Subscription Visual Studio Professional ✓ • Resource group (New) rg-wafv2 ✓ • Location North Europe ✓ • Availability zone None ✓ • Suing extra groups Vour virtual network and public IP alcress must be in the same location as your greaway, If you plan on using existing resources, paner that you select the correct	2 Settings Configure application gateway 3 Summary Review and create * Minimum scale units 2 ✓ * Subscription Visual Studio Professional ✓ * Resource group (New) rg-wafv2 ✓ Create new • • Location North Europe ✓ Availability zone None Vour virtual network and public IP address must be in the same location on using existing resources, ensure that you select the correct location.	2 Settings Configure application gateway 3 Summary Review and create * Minimum scale units 2 ✓ • Subscription Visual Studio Professional ✓ • Resource group (New) rg-wafv2 ✓ • Location North Europe ✓ Availability zone ✓ None ✓	2 Settings Configure application gateway 3 Summary Review and create • Minimum scale units · • Minimum scale units · • Subscription Visual Studio Professional • • Resource group (New) rg-wafv2 • Create new • • Location • North Europe • • Nore • Vour virtual network and public IP algrees must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.	2 Settings Configure application gateway 3 Summary Review and create • Minimum scale units 2 • • Subscription Visual Studio Professional • • Resource group (New) rg-wafv2 • • Location North Europe • Availability zone • None •			* Tier WAF V2 V
3 Summary Review and create Autoscale Manual Minimum scale units 2 Subscription Visual Studio Professional Resource group (New) rg-wafv2 Create new Location North Europe None Vor virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, subscription Visual Studio Professional Visual Stu	3 Summary Review and create Autoscale Manual Minimum scale units 2 Subscription Visual Studio Professional Resource group (New) rg-wafv2 Create new Location North Europe Nore Voru virtual network and public IP address must be in the same location as your gateway. If you plant on using existing resources, ensure that you select the correct location.	3 Summary Review and create Autoscale Autosc	3 Summary Review and create Autoscale Manual Minimum scale units Z Subscription Visual Studio Professional ✓ Subscription New) rg-wafv2 ✓ Create new Location North Europe Availability zone None Voru virtual network and public IP alcrease smust be in the same location as your speaway. If you Jano using existing resources, subscription Vour virtual network and public IP alcrease smust be in the same location as your speaway. If you Jano using existing resources, Burter and you select the correct location. Subscription	3 Summary Review and create → Minimum scale units 2 • Subscription ✓ Isual Studio Professional • Resource group (Wev) rg. wafv2 ✓ Create new • Location North Europe ✓ Availability zone Nore ✓ Voruitual network and public IP address must be in the same Isoton sy our gateway. If you Isoton sy our gateway. If you Isot	2 Settings Configure application gateway >		Capacity type
3 Summary Review and create Minimum scale units Z ✓ Subscription Visual Studio Professional ✓ Resource group (New) rg-wafv2 ✓ Create new Location North Europe ✓ Availability zone None ✓ Your virtual network and public IP alcress must be in the same location as your gateway. If you plan on using existing resources, more used the correct	3 Summary Review and create	3 Summary Review and create	3 Summary Review and create	 3 Summary Review and create * Minimum scale units 2 • Subscription Visual Studio Professional • Resource group (New) rg-wafv2 Create new • Location North Europe ✓ Availability zone None ✓ Voru virtual network and public IP address must be in the same location Image: Summary Stress <			Autoscale Manual
Review and create	Review and create Subscription Visual Studio Professional Resource group (New) rg-wafv2 Create new Location North Europe Availability zone None Vour virtual network and public IP address must be in the same location on using existing resources, ensure that you select the correct location.	Review and create Subscription Visual Studio Professional · Resource group (New) rg-wafv2 Create new Location North Europe Availability zone None Vour virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.	 Review and create Subscription Subscription Visual Studio Professional Resource group (New) rg-wafv2 Create new Location North Europe Availability zone None Vour virtual network and public IP adress must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location. 	 Review and create Subscription Subscription Visual Studio Professional Resource group (New) rg-wafv2 Create new Location North Europe Availability zone None Xour virtual network and public (P address must be in the same location on using existing resources, ensure that you select the correct location. 	3 Summary		* Minimum scale units
Subscription Visual Studio Professional Resource group (New) rg-wafv2 Create new Location North Europe Availability zone None Your virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources,	Subscription Visual Studio Professional Resource group (New) rg-wafv2 Create new Location North Europe Availability zone None Vour virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.	 Subscription Visual Studio Professional Resource group (New) rg-wafv2 Create new Location North Europe Availability zone None Vour virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location. 	 Subscription Visual Studio Professional Resource group (New) rg-wafv2 Create new Location North Europe Availability zone None Vour virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location. 	 Subscription Visual Studio Professional Resource group (New) rg-wafv2 Create new Location North Europe Availability zone None Vour virtual network and public IP address must be in the same value of the same plane that you select the correct location. 	Keview and create		2
Resource group (New) rg-wafv2 Create new Location North Europe Availability zone None Vour virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, more using existing resources, plan on using existing resources, resources that you select the correct	Resource group (New) rg-wafv2 Create new Location North Europe Availability zone None Vour virtual network and public IP address must be in the same loadress must be in the same loadressamust be in the same loadress must be in the same loadress	Resource group (New) rg-wafv2 Create new Location North Europe Availability zone None Vour virtual network and public IP address must be in the same location as your gateway, If you plan on using existing resources, ensure that you select the correct location.	 Resource group (New) rg-wafv2 Create new Location North Europe Availability zone None Your virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location. 	 Resource group (New) rg-wafv2 Create new Location North Europe Availability zone None Vour virtual network and public IP address must be in the same In on using existing resources, ensure that you select the correct Iocation. 			Subscription Visual Studio Professional
(New) rg-wafv2 Create new Create new Location North Europe Availability zone None Vour virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, plan on using existing res	(New) rg-wafv2 Create new • • Location North Europe Availability zone None Vour virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.	(New) rg-wafv2 Create new Location North Europe Availability zone None Vour virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.	(New) rg-wafv2 Create new Create new Location North Europe Availability zone None Vour virtual network and public IP adverses must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.	(New) rg-wafv2 Create new • • Location North Europe None Availability zone None Image: Straight of the same location on using existing resources, ensure that you select the correct location.			* Resource group
	* Location * Location North Europe Availability zone None Vour virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.	• Location • Location North Europe Availability zone None Vour virtual network and public IP adverse smust be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.	* Location * Location North Europe Availability zone None Vour virtual network and public IP adverses must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.	* Location * Location * Location North Europe Availability zone None Vour virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.			(New) rg-wafv2 V
North Europe Availability zone None Your virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, pandou substitution with the same that you select the correct	North Europe Availability zone None Image: State of the s	North Europe Availability zone None Your virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.	North Europe Availability zone None Image: Constraint of the same structure of the	North Europe Availability zone None Image: State of the st			* Location
Availability zone None ✓ Your virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct	Availability zone None ✓ Vour virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.	Availability zone None ✓ Your virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.	Availability zone None Your virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.	Availability zone None Vour virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.			North Europe 🗸
Your virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources,	Your virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.	Your virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.	Your virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.	Your virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.			Availability zone
Your virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct	Your virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.	Your virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.	Your virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, ensure that you select the correct location.	Your virtual network and public IP address must be in the same location as your gateway, if you plan on using existing resources, ensure that you select the correct location.			NUTE
LIMME STREET STREET	location.	location.	lecation.	location.			Your virtual network and public IP address must be in the same location as your gateway. If you plan on using existing resources, source that you called the correct

In step 2, choose the Virtual Network and subnet for the Application Gateway to reside in (remember that the subnet that the Application Gateway is created in must be empty. A small subnet is recommended for this, a /26 or /27 for example to prevent IP address wastage).

Leave the **Frontend IP configuration** as the default settings and select the required options for **Additional Settings – HTTP2 support**, **Web Application Firewall** (set to

enabled) and Firewall Mode (set to Prevention).

			_	
	1	Basics		Subnet configuration
	-	Configure basic settings	-	* Virtual network
	2	Settings Configure application gateway		* Subnet 🚯
		5 11 5 5	_	WAFSubnet (10.0.6.0/24) V
	2	Summary		Frontend IP configuration
	5	Review and create		IP address type Public Private
			- 1	* Public ID address
				Create new Use existing
				wafv2-ip
				^ Configure public IP address
				SKU 💿
				Basic
				* Idle timeout (minutes) @
				0 4
				DNS name label 🚯
				portheuropa cloudana arura com
				.nortneurope.cloudapp.azure.com
				 Assignment Dynamic Static
				Listener configuration
4				Protocol HTTP HTTPS
				* Port
				80 🗸
				Additional Settings
				* HTTP2
				Disabled Enabled
				Web application firewall
				* Firewall status
				Disabled Enabled
				* Firewall mode
				Detection Prevention
			-	
				OK

Check the summary screen in step 3 and click **Create**. This process can take up to **20 minutes**, **be patient**!



Adding a backend pool

The CloudGuard template will create an Azure VMSS for you, using the latest Marketplace image. We will use this as the backend target for the Application Gateway.

Select the Backend Pools blade of the Application Gateway

wafv2 - Backend pools				
,O Search (Ctrl+/)	🕂 Add 🛛 Refresh			
Overview	P Search backend pools			
Activity log	NAME	RULES ASSOCIATED	TARGETS	
📫 Access control (IAM)	appGatewayBackendPool	1	0	
🛷 Tags				
X Diagnose and solve problems				
Settings				
Configuration				
Web application firewall				
Backend pools				
HTTP settings				
Frontend IP configurations				
Listeners				
📩 Rules				
Health probes				
Properties				
Locks				
Automation script				
Monitoring				
Alerts				
iii Metrics				
Backend health				
Diagnostics logs				

Double click the **appGatewayBackendPool** backend pool and you have the option to add a target, as shown below.

dit backend pool		L
Save 🗙 Discard 🗴 Delete		
ame In Gatavan Packand Pack		
Remove all targets from backend pool		
rgets		
rgets backend pool can be pointed to a specific virtual	machine, virtual machine scale set, an IP address/FQDN or an app service	2.
rgets backend pool can be pointed to a specific virtual /MSS	machine, virtual machine scale set, an IP address/FQDN or an app service	2.
rgets backend pool can be pointed to a specific virtual /MSS	machine, virtual machine scale set, an IP address/FQDN or an app service	2.
rgets backend pool can be pointed to a specific virtual /MSS VMSS	machine, virtual machine scale set, an IP address/FQDN or an app service NETWORK INTERFACE CONFIGURATIONS	2.
rgets backend pool can be pointed to a specific virtual //MSS vmss cpvmss	machine, virtual machine scale set, an IP address/FQDN or an app service NETWORK INTERFACE CONFIGURATIONS eth0	<u>م</u>
rgets backend pool can be pointed to a specific virtual /MSS vmss cpvmss Select a virtual machine scale set	machine, virtual machine scale set, an IP address/FQDN or an app service NETWORK INTERFACE CONFIGURATIONS eth0 Waiting for virtual machine selection	a.
rgets backend pool can be pointed to a specific virtual /MSS vmss cpvmss Select a virtual machine scale set	machine, virtual machine scale set, an IP address/FQDN or an app service NETWORK INTERFACE CONFIGURATIONS eth0 Waiting for virtual machine selection	۵. ۱۱۰۰ ۲
rgets backend pool can be pointed to a specific virtual /MSS vmss cpvmss Select a virtual machine scale set Virtual machine scale set 'cpvmss' was added	machine, virtual machine scale set, an IP address/FQDN or an app service NETWORK INTERFACE CONFIGURATIONS eth0 Waiting for virtual machine selection 'to this backend pool. Upgrade all the instances of 'cpvmss' for this change	2.
rgets backend pool can be pointed to a specific virtual /MSS vmss cpvmss Select a virtual machine scale set Virtual machine scale set 'cpvmss' was added	machine, virtual machine scale set, an IP address/FQDN or an app service NETWORK INTERFACE CONFIGURATIONS eth0 Waiting for virtual machine selection to this backend pool. Upgrade all the instances of 'cpvmss' for this change	e.

Choose the CloudGuard VMSS as the target and add **eth0** as the network configuration (the external facing interface). You may see two VMSS entries – one per interface, make sure you use the **external** interface. Click **Save**.

Upgrading the VMSS

For the backend pool change to take effect, the VMSS must be upgraded. This restarts the VMSS instances so they are aware of the Application Gateway monitoring. Go to the VMSS in the Azure Portal, check the box next to the VMSS and click **Upgrade**. This takes around 2 minutes.

Home > Virtual machine scale sets > cpvmss - Ins	tances			
Virtual machine scale ≪ ☆ × Default Directory	cpvmss - Instances Virtual machine scale set			
🕂 Add 🛛 Edit columns 🛛 😶 More	,⊅ Search (Ctrl+/) ≪	▶ Start 🔍 Restart 🔳 Deallocate 🛛 Reimage	🛅 Delete 🔺 Upgrade	
Filter by name	🧕 Overview	✓ Search virtual machine instances		
NAME 🗈	Activity log	NAME	STATUS	LATEST MODEL
Cpvmss	Access control (IAM)	cpvmss_2	Running	🔺 No
* '	🛷 Tags			
	✗ Diagnose and solve problems			
	Settings			
	Instances			
	Scaling			
	Storage			
	Operating system			
	Size			
	Extensions			
	🐔 Continuous delivery (Preview)			
	% Identity			
	H Properties			
	Locks			
	Automation script			
	Monitoring			
	💷 Alerts			
	iii Metrics			
	Support + troubleshooting			
	New support request			

▶ Start <a>Restart <a>Deallocate <a>Chi Reimage	🛍 Delete 1 Upgrade	
${\cal P}$ Search virtual machine instances		
NAME	STATUS	LATEST MODEL
✓ cpvmss_2	Running	🔺 No

Verifying backend health

To ensure the backend VMSS is being successfully monitored by the Application Gateway, click **Backend Health** under the **Monitoring** blade of the Application Gateway.

Search (Ctrl+/)	U Refresh			
Overview	Search backend health			
Activity log	SERVER (BACKEND POOL)	PORT (HTTP SETTING)	STATUS	DETAILS
Access control (IAM)	10.0.2.4 (appGatewayBackendPool)	80 (appGatewayBackendHttpSettings)	Healthy	Success
Tags				
Diagnose and solve problems				
ttings				
Configuration				
Web application firewall				
Backend pools				
HTTP settings				
Frontend IP configurations				
Listeners				
Rules				
Health probes				
Properties				
Locks				
Automation script				
nitoring				
Alerts				
Metrics				
Backend health				

Configuring Backend HTTP Settings

It is possible to configure Application Gateway specific functionality such as Connection Draining prior to putting the gateway into use. This allows sessions to be gracefully closed when scaling operations take place.

In the backend HTTP settings, the appropriate port should be set for the gateway listener that we use for NAT traffic to a back end web service (TCP 8086 to TCP 80, in this case). This section can be found under **HTTP Settings** blade for the Application Gateway.

appGatewayBackendHttpSettings	
🔒 Save 🗙 Discard 🗴 Delete	
Name appGatewayBackendHttpSettings	
* Cookie based affinity Disabled Enabled	
* Connection draining Disabled Enabled	
Drain timeout (seconds) 🕐	60
* Protocol HTTP HTTPS * Port 0 snos	
* Request timeout	· · ·
10	✓
Override backend path	
Use for App service	•
Use custom probe 🚯	
Pick host name from backend address	

Create new TCP service in SmartConsole

The Application Gateway is configured to send traffic to a specific port (in this case 8086), so a new TCP service must be created in SmartConsole so that rules can be configured in the Check Point rule base.

Add the TCP service and set the protocol as HTTP.

	ter Object Comment
General	General ·····
Advanced	Protocol: 😵 HTTP 🔹
	foundation of data communication for the World Wide Web. Match By Port: Standard Port (80) Customize 8086 Protocol Signature is disabled ●

Configuring Access Control and NAT Rules

Add the new service to an access rule – you may need to create dynamic objects for **LocalGatewayExternal** (eth0 on the gateways) and **LocalGatewayInternal** (eth1). Using dynamic objects allows scaling without defining specific gateways.

Application Access (2)								
2	Allow App Gateway traffic to Nginx	* Any	LocalGatewayExternal	* Any	😵 tcp_8086	Accept	📄 Log	* Policy Targets
 Cleanup Rul 	es (3)							
3	Cleanup rule	* Any	* Any	* Any	* Any	Orop	🗐 Log	* Policy Targets

©2018 Check Point Software Technologies Ltd. All rights reserved | P. 8

Add a corresponding NAT rule

 Manual Lo 	▼ Manual Lower Rules (3-5)							=
3	All_Internet	💻 Internal_Windows	Remote_Deskto	♣ LocalGatewayExte	Internal_Windows	😡 rdp_remote	* Policy Targets	
4	All_Internet	✤ LocalGatewayExte	S tcp_8085	⊕ _H LocalGatewayInte	🖶 _s Nginx	🚱 http	* Policy Targets	
5 4	All_Internet	✤ LocalGatewayExte	😵 tcp_8086	⊕ _H LocalGatewayInte	🚍 _s Nginx	😚 http 🖿	* Policy Targets	

Publish and install the policy to the CloudGuard gateway(s).

Testing the connection

From a web browser, check the connection to the internal web server (shown as Nginx in the above example) using the frontend IP address of the Application Gateway, you should see the default Nginx landing page.

Troubleshooting

Ensure the backend VMSS is shown as healthy in the Application Gateway.

Verify the backend listener port is configured to the custom TCP port (8086, for example)

Check you have added an entry for the TCP service 8086

Verify the access control policy

Verify the NAT policy

Check route table entries – there should be a UDR for the internal subnet that routes all traffic (0.0.0/0) to the internal load balancer and one on the Web subnet that does the same

Ensure all Check Point changes are published and policy changes applied to gateways!

Revision History

Version	Date	<u>Comments</u>
0.1	7/11/2018	Initial draft