

# How to Configure Azure Cloud Integration Using ARM

#### https://campus.barracuda.com/doc/98210727/

Azure Cloud Integration allows the firewall to connect directly to the Azure service fabric in order to rewrite Azure user-defined routes and to monitor the IP forwarding setting of the NIC of your firewall VM.

There are two methods available for Cloud Integration. The recommended method is Managed Identity because it is easier to maintain and configure.

- Managed Identity For more information, see <u>Barracuda CloudGen Firewall Managed</u> Identities in <u>Microsoft Azure</u>.
- Service Principal (User Identity) Certificate authentication is used to authenticate the firewall when accessing the Azure API endpoints. The certificate must be valid for at least 1 year. The end date of the certificate is used by the setup script to also determine the end date for the Microsoft Entra ID application. When the certificate or the Entra ID application expires, the firewall can no longer use Azure Cloud Integration features until the Entra ID application and the corresponding certificate have been replaced. If a <u>global HTTP proxy</u> is configured, all calls to the Azure REST API are sent via the proxy.

Cloud Integration is required for the following features:

• Barracuda Firewall Admin dashboard Cloud Information element.

✓ CLOUD INFORMATION		¢
Cloud Integration	Configured	Э
Hosting Cloud	Azure	
Instance Name	CampusHACGFW	
Instance Size	Standard_F1s	
Location	westeurope	
Public IP Address	52.142.226.140	
Resource Group	Campus-HA	€
VNet/Subnet	newVirtualNetwork/FirewallSubnet	€

- UDR route rewriting for CloudGen Firewall high availability clusters
- IP forward protection

### **Before You Begin**

- You need sufficient permissions in Microsoft Azure to create a service principal in Microsoft Entegra ID.
- You need sufficient permissions in Microsoft Azure to assign permissions.
- You need a CloudGen Firewall deployed in the Microsoft Azure cloud. For more information, see <u>Microsoft Azure Deployment</u>.



## Step 1. Create the Azure Management Certificate

For the firewall to be able to connect to the Azure backend, you must create and upload a management certificate. The certificate must be valid for at least two years.

You can create such a certificate either in Barracuda Firewall Admin or on the CLI using SSH. Follow Step 1.1 to create in Firewall Admin or Step 1.2 to create on the CLI.

### Step 1.1 Create the Azure Management Certificate in Barracuda Firewall Admin

Follow this step to create the management certificate in Barracuda Firewall Admin.

- 1. Log into the firewall via Firewall Admin.
- 2. Go to CONFIGURATION > Configuration Tree > Advanced Configuration > Certificate Store.
- 3. Click Lock.
- 4. Right-click in the **Certificate Store** section.
- 5. Select Create Self Signed Certificate.

$\equiv$ $\checkmark$ + $\square$ 10.17.94.215 CA-804-Rele	ase ×			
DASHBOARD CONFIGUR/	CONTROL	FIREWALL	LOGS STATISTICS	EVENTS SSH
Configuration Tree Cert	tificate × e			
Certificate Store				
Name	Subject	Issu	er	Is CA Has Ex

Create Self Signed Certificate	
Import a new Certificate Store Entry	>
Show Filter	<ctrl q=""></ctrl>
Find	<ctrl f=""></ctrl>
Print List	
Columns	>

- 6. The Create Self Signed Certificate window opens.
- 7. Enter a name and click **Create**.

## Barracuda CloudGen Firewall



Create Self	Signed Certif	icate					
General							
Name	CampusCertif	ficate					
Comment							
Private Key							
Key Length (Bit	s)	2048		Create		Import K	ey
Key Hash	0						•
Subject - Issu	er						
Name [CN]				Country [C]			
State [ST]				Location [L]			
Org. [O]				Unit [OU]			
Email [E]				SubAltName			
Use Time Scope	-				_		
	F	rom 01.0	)1.1970		То	01.01.1970	
Properties							
Key	Value						
L							

- 8. Specify values for the following:
  - Name Enter a name.
  - **State** Enter your state.
  - **Org.** Enter your organization name.
  - **Email** Enter your email address.
  - **Country** Enter your country.
  - **Location** Enter your location.
  - **Unit** Enter your unit.

## Barracuda CloudGen Firewall



r						
Name	Campu	usCertificate				
Comment						
Private Key						
Key Length (Bit	ts)	2048	Create		Import Ke	≘y
Key Hash	NPI	MFC (2048 Bits)				▲ ▼
Subject - Issu	er					
Name [CN]	Camp	pusCGF	Country [C]	AT		
State [ST]	Vienr	na	Location [L]	Vienna		
Org. [O]	Camp	pus	Unit [OU]	3		
Email [E]	camp	ous@barracuda.com	SubAltName			
Use Time Scope	2					
		From 01.01.19	70 🔲 🔻	То	19.01.2038	
Properties						
Кеу		Value				
Fingerprint (S	ян	7C:6B:D0:78:F8:EA:97:/	AA:C1:6F:B7:25:9	F:BC:7F:	13:9A:30:73:2	в
Fingerprint (S	SH	61:6C:E2:E0:21:B0:55:E	2:91:BA:33:65:2	E:18:81:2	B:D8:3A:A8:59	9

- 9. Click OK. The Certificate Store section opens.
- 10. Click Send Changes and Activate.
- 11. In the **Certificate Store** section, double-click on the certificate you just created to expand it.
- 12. Select the first entry and right-click it.

Certificate Store				
Name	Subject	lssuer	ls CA	Has
<ul> <li>CampusCertificate</li> </ul>				0
	CampusCGF	CampusCGF	$\bigcirc$	

13. Select **Export the selected Certificate** and **to File**.



Certifica	te Store				
Name	Subject		Issuer	ls CA	Has Expires
CampusCertificate	e				<b>Ø</b>
	CCCF		CampusCGF	<b>S</b>	19.01.2038
	Show Certificate		to Clinhoord		
	Export the selected Certificate		to Ciipboard		
	Show Filter	<ctrl q=""></ctrl>	to File		
	Find	<ctrl f=""></ctrl>			
	Expand All				
	Collapse All				
	Copy List to Clipboard Copy selected to Clipboard Export to File Print List				
	Columns	>			

14. Save the certificate as a \*.cer file.

🔊 Save As			×
Save in:	Documents ~	G 🤌 📂	
Quick access Desktop Libraries This PC	Name Custom Office Templates OneNote Notebooks Snagit Zoom	Status © () () () ()	Date modified 19.11.2020 14:53 19.10.2020 15:21 19.11.2020 23:04 05.02.2021 09:41
Network	< File name: CampusCert	~	> Save
	Save as type: Certificate File (*.cer)	~	Cancel

15. Repeat the last step and save the file as \*.pem file as well.

### Step 1.2 Create the Azure Management Certificate on the CLI via SSH

Follow this step to create the management certificate using the CLI via SSH. Note: Skip this step if you already created a certificate in Barracuda Firewall Admin.

- 1. Log into the firewall via ssh.
- 2. Create the certificate:

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout arm.pem -
out arm.pem
```



- 3. Answer the questions at the prompt. The **Common Name** is used to identify this certificate in the Azure web interface.
- 4. Convert the certificate to CER, as required by Azure:

```
openssl x509 -inform pem -in arm.pem -outform der -out arm.cer
```

5. Extract the RSA key:

```
openssl rsa -in arm.pem -out arm.key.pem
```

You now have three certificates: *arm.pem*, *arm.key.pem* and *arm.cer*. Use the download function to save these somewhere safe on your device.

### Step 2. Create a Microsoft Azure Service Principal

Create a service principal in Microsoft Azure and configure to authenticate with a certificate.

- 1. Log into the Azure portal: <u>https://portal.azure.com</u>
- 2. In the left menu of the Microsoft Entra ID blade, click App registrations.
- 3. Click New registration.



- 4. The **Register an application** blade opens. Specify values for the following:
  - **Name** Enter a name for the application registration.
  - Supported account types Select Accounts in this organizational directory only (<your\_directory\_name> only - Single tenant). If you have multiple Microsoft Entegra ID accounts, select Accounts in any organizational directory - Multitenant).
  - **Redirect URI** (optional) Leave this field blank.



#### Register an application

The user-facing display name for this application (this can be changed later).	
BarracudaCGFApp	~
Supported account types	
Who can use this application or access this API?	
Accounts in this organizational directory only (cudazure only - Single tenant)	
Accounts in any organizational directory (Any directory - Multitenant)	
O Accounts in any organizational directory (Any directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)	
Help me choose	
Redirect URI (optional)	
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional an changed later, but a value is required for most authentication scenarios.	d it can be
Web V e.g. https://example.com/auth	

- 5. Click **Register**.
- 6. The newly registered application opens automatically when it is finished.
- 7. In the left menu, click **Certificates & secrets** .

Home > cudazure >	
BarracudaCGFApp	\$ <sup>2</sup> ···
	📋 Delete 🌐 Endpoints
Overview	🚺 Got a second? We would
🝊 Quickstart	developer).
💉 Integration assistant	∧ Essentials
Manage	Display name BarracudaCGFApp
🔤 Branding	Application (client) ID
Authentication	Directory (tenant) ID
📍 Certificates & secrets	
Token configuration	Object ID

8. In the Certificates & secrets blade, click Upload certificate .



« 💛 Got feedback?			
Credentials enable confidential ap	plications to identify themselv	es to the authentication	service when
receiving tokens at a web address we recommend using a certificate	able location (using an HTTPS (instead of a client secret) as	scheme). For a higher le a credential.	vel of assurance
Certificates			
Certificates can be used as secrets referred to as public keys.	to prove the application's ide	ntity when requesting a	token. Also can
_			
↑ Upload certificate			
Thumbprint	Start date	Expires	ID
	Credentials enable confidential ap receiving tokens at a web address we recommend using a certificate Certificates Certificates can be used as secrets referred to as public keys.	Credentials enable confidential applications to identify themselv receiving tokens at a web addressable location (using an HTTPS we recommend using a certificate (instead of a client secret) as Certificates Certificates Certificates can be used as secrets to prove the application's ide referred to as public keys.	Credentials enable confidential applications to identify themselves to the authentication receiving tokens at a web addressable location (using an HTTPS scheme). For a higher le we recommend using a certificate (instead of a client secret) as a credential. Certificates Certificates Certificates can be used as secrets to prove the application's identity when requesting a referred to as public keys. Upload certificate Thumbprint Start date Expires

9. The Upload Certificate window opens. Select the \*.cer file created in Step 1 and click Add .
 10. After the upload is complete, the certificate is displayed in the list.

Home > cudazure > BarracudaCGFApp

🛉 BarracudaCGFAp	p	Certificates & secrets 🛛 🛪	·		×			
	~	♡ Got feedback?						
Overview		Credentials enable confidential applications	to identify themsel	ves to the authentication	service when			
🗳 Quickstart		receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assuranc we recommend using a certificate (instead of a client secret) as a credential.						
💉 Integration assistant								
Manage		Certificates						
🔤 Branding		Certificates can be used as secrets to prove referred to as public keys.	the application's ide	entity when requesting a t	oken. Also can be			
Authentication								
📍 Certificates & secrets		↑ Upload certificate						
Token configuration		Thumbprint	Start date	Expires	ID			
API permissions		69A132B4CB4300063400FB1BB0330	1/1/1970	1/19/2038	2bcf87c7-7			
Expose an API		•			+			
App roles   Preview								

- 11. Click Overview .
- 12. In the **Overview** blade, copy the **Application (client) ID** and the **Directory (tenant) ID** and insert both into a text editor. You will need this information later.



BarracuuaCGFA		
	« 📋 Delete 🜐 Endpoints 💀 Previev	v features
Overview	∧ Essentials	
🗳 Quickstart	Display name	: BarracudaCGFApp
Integration assistant	Application (client) ID	:
, megradon assistant	Directory (tenant) ID	:
Manage	Object ID	:
Branding	Supported account types	: My organization only
Authentication	Redirect URIs	: Add a Redirect URI
Certificates & secrets	Application ID URI	: Add an Application ID URI
	Managed application in local directory	: BarracudaCGFApp

### Step 3. Assigning the Permissions

- 1. Go to the Azure portal: https://portal.azure.com
- 2. G o to the Resource Group that contains the VNET and User Defined Routes of the CloudGen Firewall.
- 3. In the left menu, select Access Control (IAM).

Dashboard > Campus-CGF-VNET



- 4. Click + Add.
- 5. Select Add role assignment.



#### Dashboard > Campus-CGF-VNET

Reampus-CGF-VNET	Access control (IAM)
✓ Search (Ctrl+/) «	$+$ Add $\downarrow$ Download role assignments $\equiv\equiv$ Edit columns $\circlearrowright$
<ul> <li>↔ Overview</li> </ul>	Add role assignment
Activity log	Add co-administrator
Access control (IAM)	My access
🗳 Tags	View my level of access to this resource.
Diagnose and solve problems	View my access
Settings	<b>Check access</b> Review the level of access a user, group, service principal, or
↔ Address space	managed identity has to this resource. Learn more 🖻
${\mathscr S}$ Connected devices	Find ①
<-> Subnets	User, group, or service principal
DDoS protection	Search by name or email address

- 6. The Add role assignment window opens. Specify values for the following:
  - Role Select Network Contributor.
  - Assign Access to Select User, group, or service principal.
  - **Select** Enter the name of the application created in Step 2 and click on its entry in the list.

Add role assignment  $\times$ 

Role 🕕	
Network Contributor 🛈	$\sim$
Assign access to 🕕	
User, group, or service principal	$\sim$
Select 🛈	
barracudaCGFApp	

No users, groups, or service principals found.

0	Selected men	ibers:	
	Bar	racudaCGFApp	Remove
	Save	Discard	

7. Click Save.

This role is sufficient for the firewall to manage the route tables. If you want the firewall to monitor



the IP Forwarding setting of its network interfaces as well, you must add the role **Virtual Machine Contributor**. Repeat Step 3 and select **Virtual Machine Contributor**.

~
~
$\checkmark$
Remove

## Step 4. Get the Subscription ID

- 1. Log into the Azure portal: <u>https://portal.azure.com</u>
- 2. In the left menu, click **Subscriptions**.
- 3. Copy the **Subscription ID** in the **Subscription ID** column. Home > Subscriptions >



 Insert the Subscription ID in the text editor where you already inserted the Application (client) ID and the Directory (tenant) ID. You will need these 3 IDs in the Step 5.



### Step 5. Configure Cloud Integration on the Firewall

- 1. Log into the firewall via Firewall Admin.
- 2. Go to **CONFIGURATION > Configuration Tree > Cloud Integration**.
- 3. Click Lock.
- 4. In the left menu, click **Azure Networking**.
- 5. In the Azure Networking section, specify values for the following:
  - Azure Deployment Type Select Azure Resource Manager.
  - **Subscription ID** Enter your Subscription ID, retrieved in Step 4.
  - Tenant ID Enter your Tenant ID, retrieved in Step 2.
  - **Application ID** Enter your Application ID, retrieved in Step 2.
  - Resource Group Enter the name of the resource group containing the VNET and the UDR route table.
  - Virtual Network Name Enter the name of the virtual network.
  - Select Certificate Select the certificate created in Step 1 from the drop-down list.
  - Management Key Click on the settings icon. Select Import from File and select the \*.pem file created in Step 1.
  - Protect IP forward settings Select yes.

Azure Networking		
Azure Deployment Type	Azure-Resource-Manager-(ARM)	<b>.</b> ~
Subscription ID		Ē~
Tenant ID		Ē~
Application ID		Ē.~
Resource Group	catamaniuk-RG-CGF	Ē~
Virtual Network Name	catamaniukCGF-VNET	Ē~
Route Check Interval	300	Ē~
Select certificate	CampusCGF 🔹 🔿	
Management Key	Hash: FMDJGQ 2048 Bits	
Protect IP forwarding settings	yes 🗸	<b>.</b>

6. Click Send Changes and Activate.

Anura Naturalia

### Step 6. Configure Azure Environment

If your firewall is running in a non-default Azure environment, such as Azure Germany, govcloud , Azure China, or Azure Stack, you must configure the Azure environment. Otherwise, you can skip this step.



- 1. Log into the firewall via Firewall Admin.
- 2. Go to **CONFIGURATION > Configuration Tree > Cloud Integration**.
- 3. Click Lock.
- 4. In the left menu, click **Configuration mode** and click **Switch to Advanced**.
- 5. In the left menu, click **Azure Networking**.
- 6. Then, specify values for the following:
  - Azure Environment Select the Azure Environment from the drop-down menu. Select Explicit if your environment is not listed in the drop-down menu. If you have selected Explicit, you must provide the following configuration:
  - Service Management URL Enter the Service Management URL.
  - Resource Manager URL Enter the Resource Manager URL.
  - Active Directory Authority Enter the Active Directory Authority.
  - **Token Issuer Service URL** Enter the Token Issuer Service URL.
  - **Resource** Enter the resource identifier.

Azure Networking	Azure Deployment Type	Azure-Resource-Manager-(ARM)	✓
Azure Event Hub	Subscription ID		Ēv
Azure OMS Azure Virtual WAN	Tenant ID		Ē
AWS Integration AWS Cloudwatch	Application ID		
AWS Autoscaling	Resource Group	catamaniuk-RG-CGF	Ēv
	Virtual Network Name	catamaniukCGF-VNET	Ē
<ul> <li>Configuration Mode</li> <li>Switch to Basic View</li> </ul>	Route Check Interval	300	Ēř
	Select certificate	CampusCGF	▼ ⊖
	Management Key	Hash:	¢.~
	Management Key Protect IP forwarding settings	Hash: yes	<b>☆</b> ~ ▼ ≣-
	Management Key Protect IP forwarding settings I Azure Environment	Hash: yes Germany	Ç.~ 
	Management Key Protect IP forwarding settings I Azure Environment I Service Management URL	Hash: yes Cermany https://management.core.windows.net	\$
	Management Key Protect IP forwarding settings I Azure Environment I Service Management URL I Resource Manager URL	Hash: yes Cermany https://management.core.windows.net https://management.azure.com	** = = = = = = = = = = = = =
	Management Key Protect IP forwarding settings Azure Environment Service Management URL Resource Manager URL Active Directory Authority	Hash: yes Cernany Inttps://management.core.windows.net Inttps://management.azure.com Inttps://login.windows.net	
	Management Key Protect IP forwarding settings I Azure Environment I Service Management URL I Resource Manager URL I Active Directory Authority I Token Issuer Service URL	Hash: yes Cermany https://management.core.windows.net https://management.azure.com https://login.windows.net https://sts.windows.net	

7. Click Send Changes and Activate.

### Monitoring

Go to **NETWORK > Azure UDR** to see the UDR routing table for all subnets in the firewall's VNET. Routes using the firewall VM as the next hop are marked with a green icon. This icon changes to red during the UDR HA failover process.



Interfaces/IPs IPs Ir	nterfaces	Proxy ARPs	ARPs	Statistics	OSPF	RIP	BGP	Switch Info	IPv6 ND Cache	e Azure UDR	]
Table / Route		Prefix				Next	Нор Тур	e	N	lext Hop Gatew	ay Mode
DOC-Routetab	le										
Backend-2-I	INET	0.0.0/				Virtu	ual Appliar			10.8.1.10	ARM

### All activity is logged to the **Box\Control\daemon** log file.

Box\Control\daemon <new log=""></new>						
Select Log File	Box\Co	ontrol\daemon		✓ Reload Log File Tree		
Time		Туре	TZ	Message		
2016 01 22 10:1	12:17	Notice	+00:00	control: UDP Handler: Server/Service state changed		
2016 01 22 10:1	12:21	Notice	+00:00	Server State Changed		
2016 01 22 10:1	12:21	Info	+00:00	Server State for VSNGFHA: this=down other=secondary		
2016 01 22 10:1	12:21	Notice	+00:00			
2016 01 22 10:1	12:21	Notice	+00:00	Public Key for secondary boxIP 10.8.1.20 server VSNGFHA present		
2016 01 22 10:1	12:32	Info	+00:00	control: Send session poll request status to master 10.8.10.10		
2016 01 22 10:1	12:35	Notice	+00:00	control: UDP Handler: Server/Service state changed		
2016 01 22 10:1	12:35	Info	+00:00	control: Send status poll request status to master 10.8.10.10		
2016 01 22 10:1	12:35	Info	+00:00	control: Send session poll request status to master 10.8.10.10		
2016 01 22 10:1	12:36	Info	+00:00	control: route Backend-2-INET in route table DOC-Routetable successfully updated (old gateway IP: 10.8.1.20 new gateway IP: 10.8.1.10)		



### Figures

- 1. dashboard\_Cl.png
- 2. create\_cert.png
- 3. create2.png
- 4. cert3.png
- 5. export1.png
- 6. export2.png
- 7. export3.png
- 8. app\_reg\_new.png
- 9. register\_new\_app.png
- 10. cert\_sec.png
- 11. upload\_cer.png
- 12. upload\_success.png
- 13. ids.png
- 14. IAM1.png
- 15. add\_ra.png
- 16. add\_role1.png
- 17. add\_role2.png
- 18. copy\_sub\_id.png
- 19. cloud\_integration.png
- 20. azure\_env.png
- 21. ARM-UDR\_01.png
- 22. ARM-UDR\_02.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.