How to Configure Azure Cloud Integration using ASM

https://campus.barracuda.com/doc/48202629/

Azure Cloud integration allows the firewall to connect directly to the Azure service fabric to rewrite Azure User Defined Routes and to monitor the IP Forwarding setting of the NIC of your firewall VM. Azure User Defined Routing allows you to use the Firewall F-Series high availability cluster in the frontend subnet as the default gateway for all your VMs running in the backend networks. You must enable IP Forwarding for the firewall VMs and create and apply an Azure routing table to the backend networks. Using a management certificate and the Azure subscriber ID, the firewall VMs can change the Azure routing table on the fly when the virtual server fails over from one VM to the other. Azure route table rewriting must be configured on the primary and secondary F-Series Firewall. Multiple network interfaces are not supported. If a global HTTP proxy is configured, all REST API calls are sent via the proxy.

Before you begin

- Deploy your F-Series firewall, and configure Azure UDR using **Azure Service Manager**. For more information, see How to Configure Azure Route Tables (UDR) in Azure using PowerShell and ASM.
- Install Azure PowerShell.
- Verify that a DNS server is configured. For more information, see How to Configure DNS Settings

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 one year.

1. Log into the NextGen Firewall F-Series via ssh.
2. Create the certificate:
   openssl req -x509 -nodes -days 730 -newkey rsa:2048 -keyout mycert.pem -out mycert.pem
   `openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout mycert.pem -out mycert.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 mycert.pem -outform der -out mycert.cer
   `openssl x509 -inform pem -in mycert.pem -outform der -out mycert.cer`

If you are using an OpenSSL version that generates PKCS#8 keys, you must extract the RSA key separately:

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

In this case, upload mycert.pem as the Azure **Management Certificate** and mycert.key.pem as the **Management Key** on the firewall.

You now have two certificates: mycert.pem and mycert.cer.

Step 3. Upload the Azure management certificate

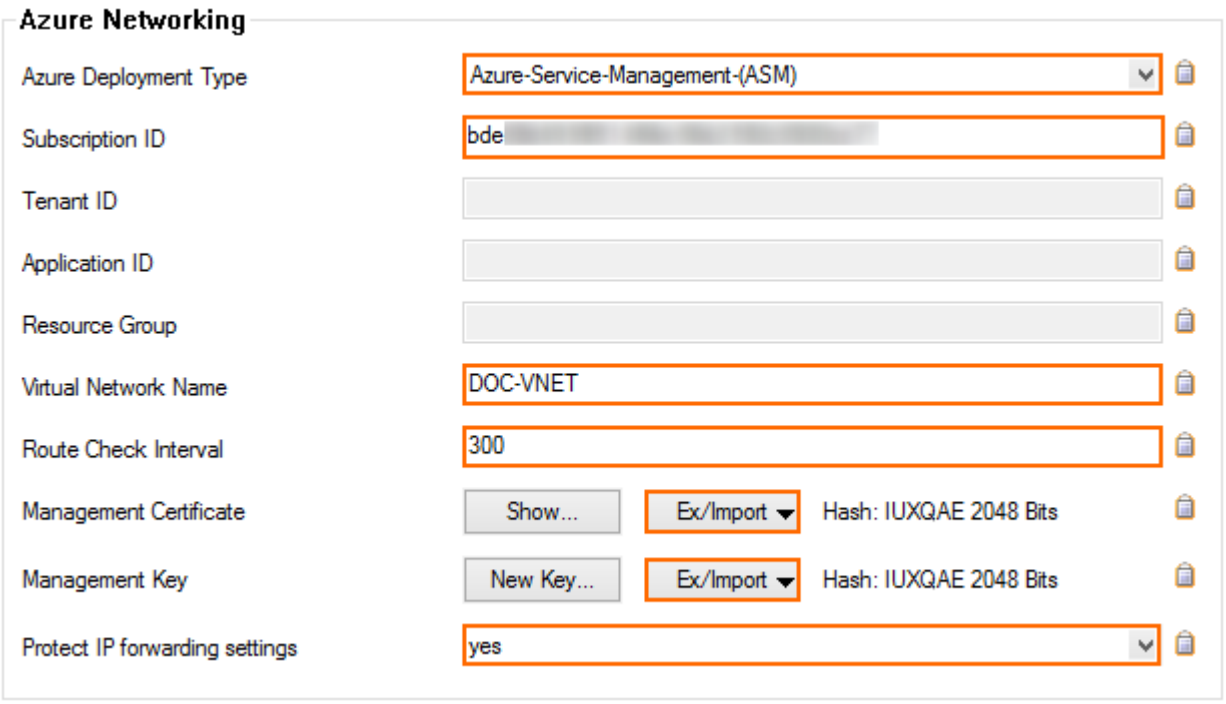
1. Log into the Microsoft Azure Management Portal (https://manage.windowsazure.com).
2. On the bottom of the left menu, click on **SETTINGS**.
3. In the top navigation, click on **MANAGEMENT CERTIFICATES**.
4. On the bottom, click **UPLOAD.**
5. Select the *mycert.cer* certificate created in Step 2, and click **OK**.

The management certificate is now listed with the **Common Name** of the certificate used as the **Name**.

Step 4. Configure cloud integration

You must enter your Azure SubscriptionId, VNET name, and the management certificate to allow the firewall to connect to the Azure service fabric.

1. Go to **CONFIGURATION > Configuration Tree > Box > Advanced Configuration > Cloud Integration**.
2. Click **Lock**.
3. In the left menu, click **Azure Networking**.
4. Select **Azure Service Management (ASM)** from the **Azure Deployment Type** drop-down list.
5. Enter your Azure **Subscription ID**. Use `Get-AzureSubscription` in Azure PowerShell to display your SubscriptionId.
6. Enter the **Virtual Network Name**.
7. Next to **Management Certificate,** click **Ex/Import** and select **Import from PEM File**. The **File browser** window opens.
8. Select the *mycert.pem* certificate created in Step 2, and click **Open**.
9. Next to **Management Key** click **Ex/Import** and select **Import from File**. The **File browser** window opens.
   Select the *mycert.pem* certificate created in Step 2, and click **Open**.
   > If you are using an OpenSSL version that generates PKCS#8 keys, import the *mycert.key.pem* file as the **Management Key** on the firewall.
10. From the **Protect IP Forwarding Settings** list, select **yes** to monitor the **IP Forwarding** setting of the NIC attached to your firewall VM.

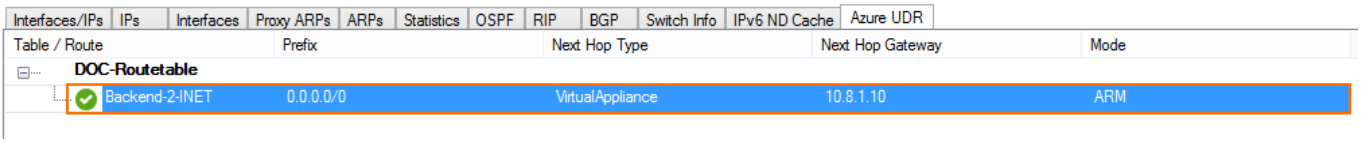


11. Click **Send Changes** and **Activate**.

The Azure routing table and the IP Forwarding settings are now monitored. If used in a HA cluster, the routes in the Azure route table are rewritten when the virtual server fails over.

Monitoring

Go to **NETWORK > Azure UDR** to see the UDR routing table for all subnets in the firewalls VNET. The green status icon is displayed for routes where the destination is a F-Series firewall. The icon changes to a red icon when a HA failover is in progress.



Log file

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

Box\Control\daemon <new Log>

Select Log File Box\Control\daemon Reload Log File Tree

Time	Type	TZ	Message
2016 01 22 10:12:17	Notice	+00:00	control: UDP Handler: Server/Service state changed
2016 01 22 10:12:21	Notice	+00:00	---------- Server State Changed ----------
2016 01 22 10:12:21	Info	+00:00	----- Server State for VSNGFHA: this=down other=secondary
2016 01 22 10:12:21	Notice	+00:00	----------
2016 01 22 10:12:21	Notice	+00:00	Public Key for secondary boxIP 10.8.1.20 server VSNGFHA present
2016 01 22 10:12:32	Info	+00:00	control: Send session poll request status to master 10.8.10.10
2016 01 22 10:12:35	Notice	+00:00	control: UDP Handler: Server/Service state changed
2016 01 22 10:12:35	Info	+00:00	control: Send status poll request status to master 10.8.10.10
2016 01 22 10:12:35	Info	+00:00	control: Send session poll request status to master 10.8.10.10
2016 01 22 10:12:36	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. UDR_HA_ASM.png
2. ARM-UDR_01.png
3. ARM-UDR_02.png