

How to Configure Azure Route Table Rewriting for HA Clusters using ASM

<https://campus.barracuda.com/doc/47579392/>

Azure User Defined Routing allows you to use the NextGen 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 F-Series VMs and create and apply an Azure routing table to the backend networks. Using a management certificate and the Azure subscriber ID, the F-Series VMs can change the Azure routing table on the fly when the virtual server fails over from one VM to the other. Azure UDR only works when using an HA cluster with one network interface. Azure Multi NIC is not supported.

In this article:

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 User Defined Routing

You must enter your Azure SubscriptionId, VNET name, and the management certificate to allow the firewall to change the Azure User Defined Routing Table.

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. Click **Lock**.
3. In the left menu, expand the **Configuration Mode** section and click on **Switch to Advanced View**.
4. In the left menu, click **Azure Networking**.
5. Select **Azure Service Management (ASM)** from the **Azure Deployment Type** drop-down list.
6. Enter your Azure **Subscription ID**. Use `Get-AzureSubscription` in Azure PowerShell to display your SubscriptionId.
7. Enter the **Virtual Network Name**.
8. Next to **Management Certificate**, click **Ex/Import** and select **Import from PEM File**. The **File browser** window opens.
9. Select the `mycert.pem` certificate created in Step 2, and click **Open**.
10. 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.

Azure Networking

! *To activate these changes, only a Soft activation is required.*

Azure Deployment Type	Azure-Service-Management-(ASM) ▼	📄
Subscription ID	bde58b49-9951-466e-90e2-592c0920ce77	📄
Tenant ID		📄
Application ID		📄
Resource Group		📄
Virtual Network Name	wideVNET	📄
Route Check Interval	300	📄
Management Certificate	<input type="button" value="Show..."/> <input type="button" value="Ex/Import ▼"/> Hash: UOAEJX 2048 Bits	📄
Management Key	<input type="button" value="New Key..."/> <input type="button" value="Ex/Import ▼"/> Hash: UOAEJX 2048 Bits	📄

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

Step 5. Perform a Soft Network Activation

1. Go to **CONTROL > Box**.
2. In the left menu, expand the **Network** section and click **Activate new network configuration**.
3. Click **Soft**.

The Azure routing table is now updated every time the virtual server fails over.

Monitoring

Go to **NETWORK > Azure UDR** to see the UDR Routing table for all subnets in the firewalls VNET. A green status icon before the route where the destination is a F-Series firewall. A UDR HA failover in progress is visualized by a red icon.

Interfaces/IPs										Azure UDR	
Table / Route	Prefix	Next Hop Type	Next Hop Gateway	Mode							
DOC-Routetable											
Backend-2-INET	0.0.0.0/0	VirtualAppliance	10.8.1.10	ARM							

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

© Barracuda Networks Inc., 2019 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.