

---

## Best Practice - Azure Public Cloud

<https://campus.barracuda.com/doc/48202835/>

Configuring a Barracuda NextGen Firewall F-Series in the Azure cloud requires you to adapt setup procedures according to the requirements and restrictions of the cloud.

### Use automatically filled custom external network objects

---

The Barracuda NextGen Firewall F-Series automatically fills the custom external network objects with network information acquired from the Azure cloud:

- Custom external object number 1 contains the internal IP address.
- Custom external object number 2 contains the internal network address.
- Custom external object number 3 contains the external IP address.

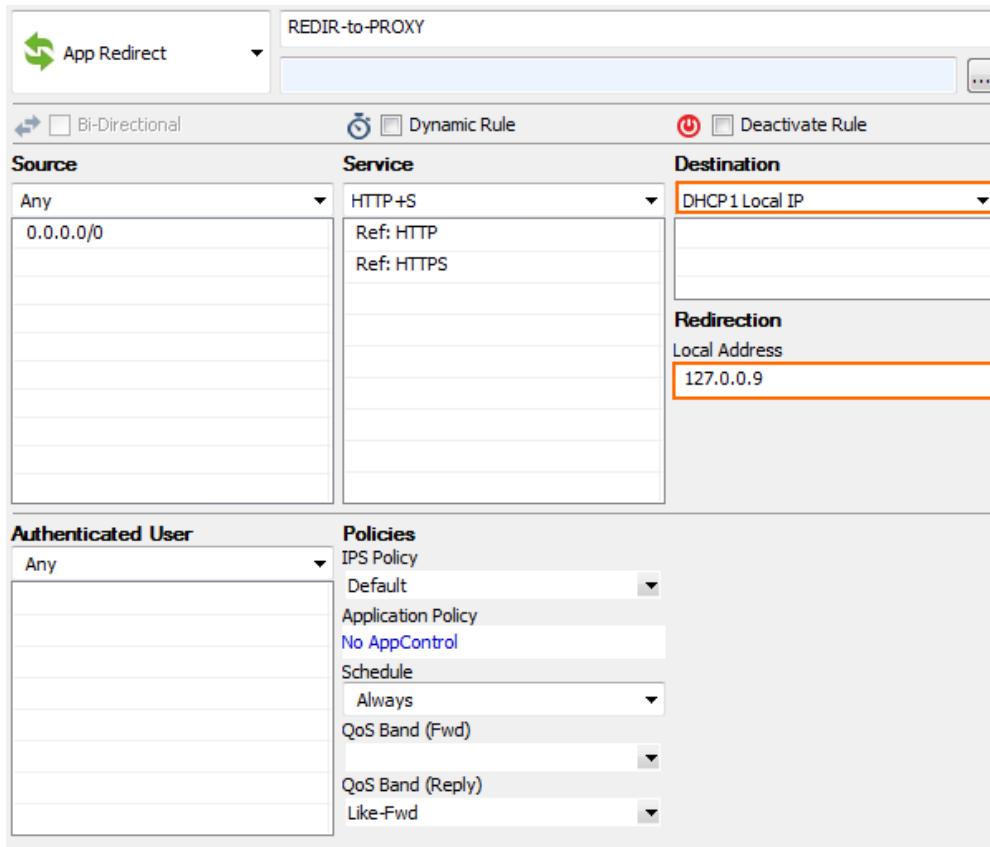
For more information, see [Custom External Network Objects](#).

### Configuring service listeners and app redirect access rules in Azure

---

#### Stand-alone firewalls

Stand-alone firewalls use one dynamic interface. The management IP address, the virtual server, and the services running on it listen on the loopback interface IP addresses. Incoming traffic on the dhcp interface must be redirected with app redirect access rules to the respective service. Use the **CONTROL > Resources** page to check the listeners for each service.

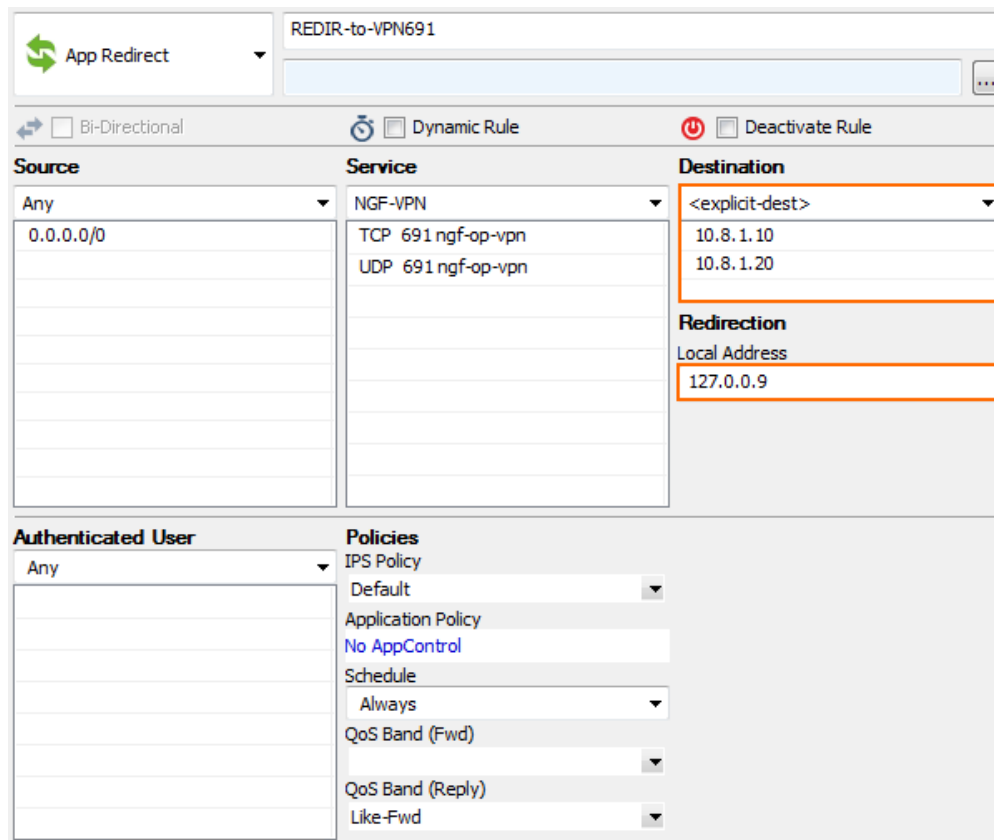


The screenshot shows the configuration for an 'App Redirect' rule named 'REDIR-to-PROXY'. The rule is configured with the following settings:

- Source:** Any (0.0.0.0/0)
- Service:** HTTP+S (References: HTTP, HTTPS)
- Destination:** DHCP1 Local IP
- Redirection:** Local Address 127.0.0.9
- Authenticated User:** Any
- Policies:**
  - IPS Policy: Default
  - Application Policy: No AppControl
  - Schedule: Always
  - QoS Band (Fwd):
  - QoS Band (Reply):
  - Like-Fwd:

### High availability clusters

High availability clusters must use static IP addresses as the management interface. Since Azure does not support floating IP addresses, the app redirect rule must match for the management IP addresses of both firewalls as the destination. Use **Any** (not **Internet**) as the source to also enable connections from other clients in the virtual network.



The screenshot shows the configuration for an 'App Redirect' rule named 'REDIR-to-VPN691'. The rule is not bi-directional, is a dynamic rule, and is active. The configuration is as follows:

Source	Service	Destination
Any	NGF-VPN	<explicit-dest>
0.0.0.0/0	TCP 691 ngf-op-vpn	10.8.1.10
	UDP 691 ngf-op-vpn	10.8.1.20

Redirection Local Address: 127.0.0.9

Authenticated User	Policies
Any	IPS Policy: Default
	Application Policy: No AppControl
	Schedule: Always
	QoS Band (Fwd):
	QoS Band (Reply):
	Like-Fwd:

## Special considerations for the VPN service IKEv1 IPsec listener

By default, the IPsec service listens on 0.0.0.0. This causes problems when used in combination with an app redirect rule because incoming traffic uses the host firewall and outgoing traffic is routed via the app redirect rule.

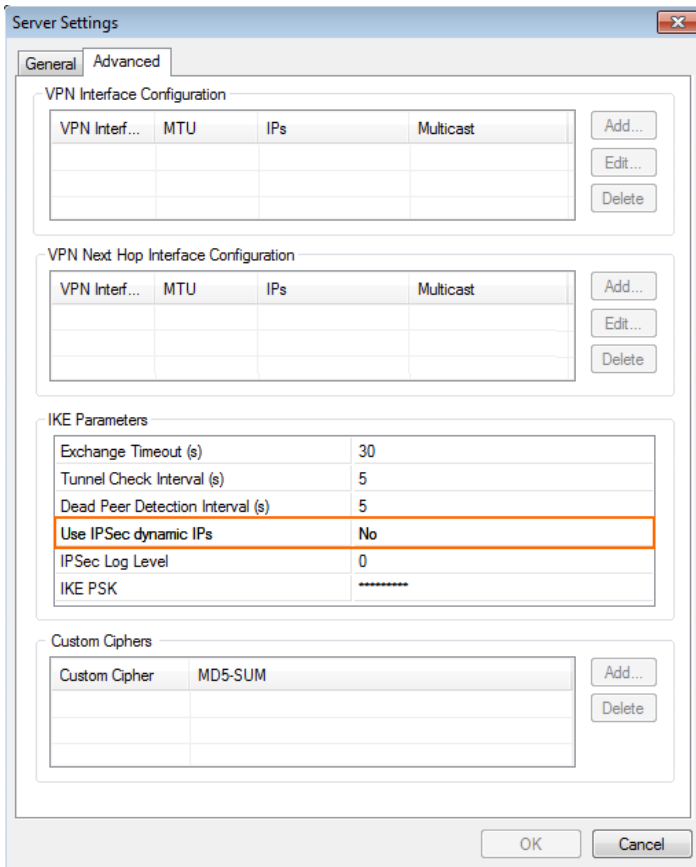
### Step 1. Configure client-to-site or site-to-site IPsec VPN

Configure an IKEv1 client-to-site or site-to-site IPsec VPN.

For more information, see [Client-to-Site VPN](#) or [Site-to-Site VPN](#).

### Step 2. Disable IPsec dynamic IP setting

Open the **VPN Settings - Server Settings** and, in the **Advanced** tab, change **Use IPsec dynamic IPs** to **No**. This disables the 0.0.0.0 listener for the ike3 (IPsec IKEv1) daemon.



The **Server Settings** dialog box is shown with the **Advanced** tab selected. It contains several configuration sections:

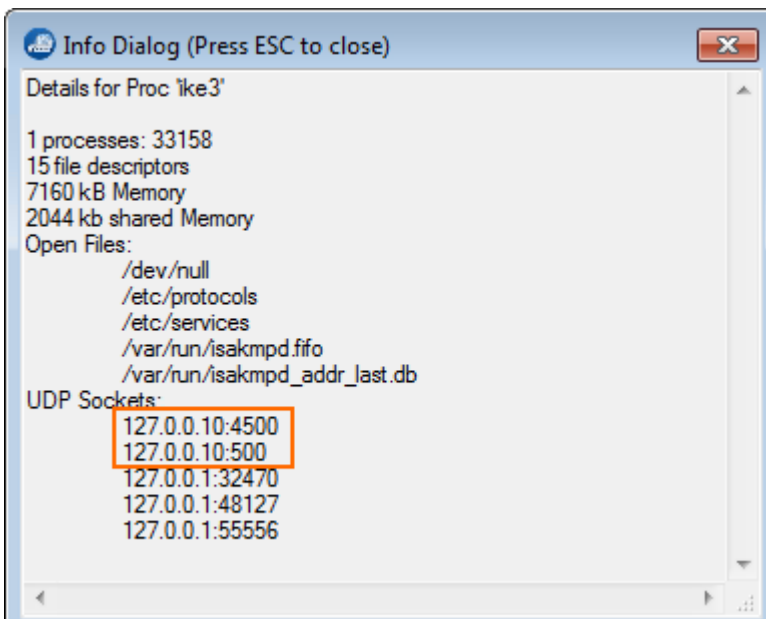
- VPN Interface Configuration:** A table with columns for VPN Interface, MTU, IPs, and Multicast. Buttons for Add, Edit, and Delete are on the right.
- VPN Next Hop Interface Configuration:** A similar table with buttons for Add, Edit, and Delete.
- IKE Parameters:** A table with the following values:

Exchange Timeout (s)	30
Tunnel Check Interval (s)	5
Dead Peer Detection Interval (s)	5
Use IPSec dynamic IPs	No
IPSec Log Level	0
IKE PSK	*****
- Custom Ciphers:** A table with one entry: Custom Cipher: MD5-SUM. Buttons for Add and Delete are on the right.

At the bottom are **OK** and **Cancel** buttons.

### Step 3. Verify ike3 listeners

Open the **CONTROL > Resources** page and double-click on the **ike3 / Tina VPN** process. Verify that the **ike3** and **Tina VPN** processes are listening only on 127.0.0.9: UDP 500 and 4500.

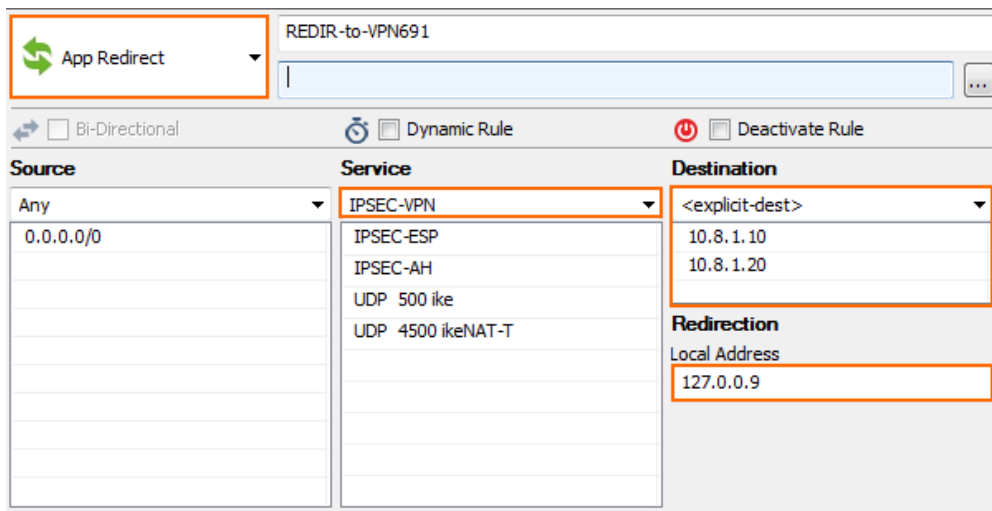


The **Info Dialog (Press ESC to close)** shows details for the **Proc 'ike3'**:

- 1 processes: 33158
- 15 file descriptors
- 7160 kB Memory
- 2044 kB shared Memory
- Open Files:
  - /dev/null
  - /etc/protocols
  - /etc/services
  - /var/run/isakmpd.fifo
  - /var/run/isakmpd\_addr\_last.db
- UDP Sockets:
  - 127.0.0.10:4500
  - 127.0.0.10:500
  - 127.0.0.1:32470
  - 127.0.0.1:48127
  - 127.0.0.1:55556

#### Step 4. Create app redirect access rule

Create an app redirect access rule to forward incoming traffic to the ikev1 daemon listening on the loopback interface. For stand-alone firewalls, use dhcp as the destination. For HA clusters, use both the primary and secondary firewall management IP address as the destination.



The screenshot shows the configuration for an 'App Redirect' rule named 'REDIR-to-VPN691'. The rule is configured with the following settings:

- Source:** Any (0.0.0.0/0)
- Service:** IPSEC-VPN (includes IPSEC-ESP, IPSEC-AH, UDP 500 ike, and UDP 4500 ikeNAT-T)
- Destination:** <explicit-dest> (includes 10.8.1.10 and 10.8.1.20)
- Redirection:** Local Address 127.0.0.9

Additional options shown include 'Bi-Directional' (unchecked), 'Dynamic Rule' (checked), and 'Deactivate Rule' (unchecked).

## Restoring a PAYG NextGen Firewall F-Series from a PAR file

Since the PAYG licenses are generated only on the first boot, extra care must be taken to not replace these licenses when using a PAR file to restore the configuration of another NextGen Firewall F-Series.

#### Step 1. Create PAR file

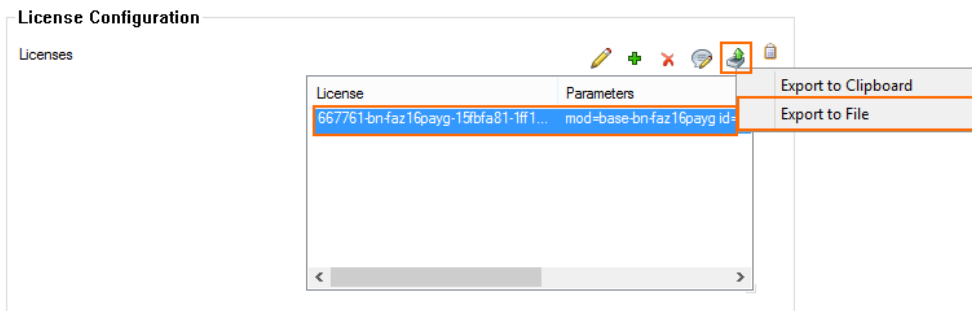
On the source PAYG NextGen Firewall F-Series, create a PAR file.

For more information, see [How to Back Up and Restore Your Systems](#) or [How to Create PAR or PCA Files on the Command Line](#).

#### Step 2. Export PAYG license on new firewall VM

On the destination PAYG NextGen Firewall F-Series, export the PAYG licenses to a file to be able to restore them later.

1. Go to **CONFIGURATION > Configuration Tree > Box Licenses**.
2. Click **Lock**.
3. Select the license in the **Licenses** list, click the export icon, and select **Export to File**.

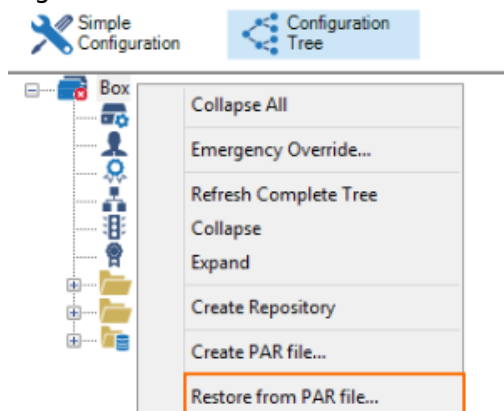


4. Save the lic file.
5. Click **Unlock**.

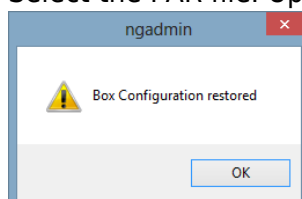
### Step 3. Restore from PAR

Restore the configuration from the PAR file. But before activating, replace the license with the license file exported in step 2.

1. Go to **CONFIGURATION > Configuration Tree**.
2. Right-click on **Box** and select **Restore from PAR File**.



3. Select the PAR file. Upon completion, the **Box Configuration restored** pop-up window opens.



4. Go to **CONFIGURATION > Configuration Tree > Box Licenses**.
5. Delete all licenses in the **Licenses** list.
6. Click **+** and select **Import from File**.
7. Select the license file you exported in step 2.
8. Click **OK** and **agree** to the end user licensing agreement.
9. Click **Send Changes** and **Activate**.
10. Go to **CONTROL > Box**.
11. If necessary, click **Activate new network configuration** and select **Failsafe** from the pop-up window.

You can now use the new PAYG image with the configuration included in the PAR file.

## Figures

1. BP\_Azure\_01.png
2. BP\_Azure\_01a.png
3. BP\_Azure02.png
4. BP\_Azure03.png
5. BP\_Azure\_04.png
6. export\_01.png
7. export\_02.png
8. export\_03.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.