Best Practice - Service Configurations in the Public Cloud

https://campus.barracuda.com/doc/73718981/

Configuring a Barracuda CloudGen Firewall in the public cloud requires you to adapt setup procedures according to the requirements and restrictions of the cloud.

Use Automatically Filled Custom External Network Objects

The firewall automatically fills the custom external network objects with network information acquired directly from the cloud provider:

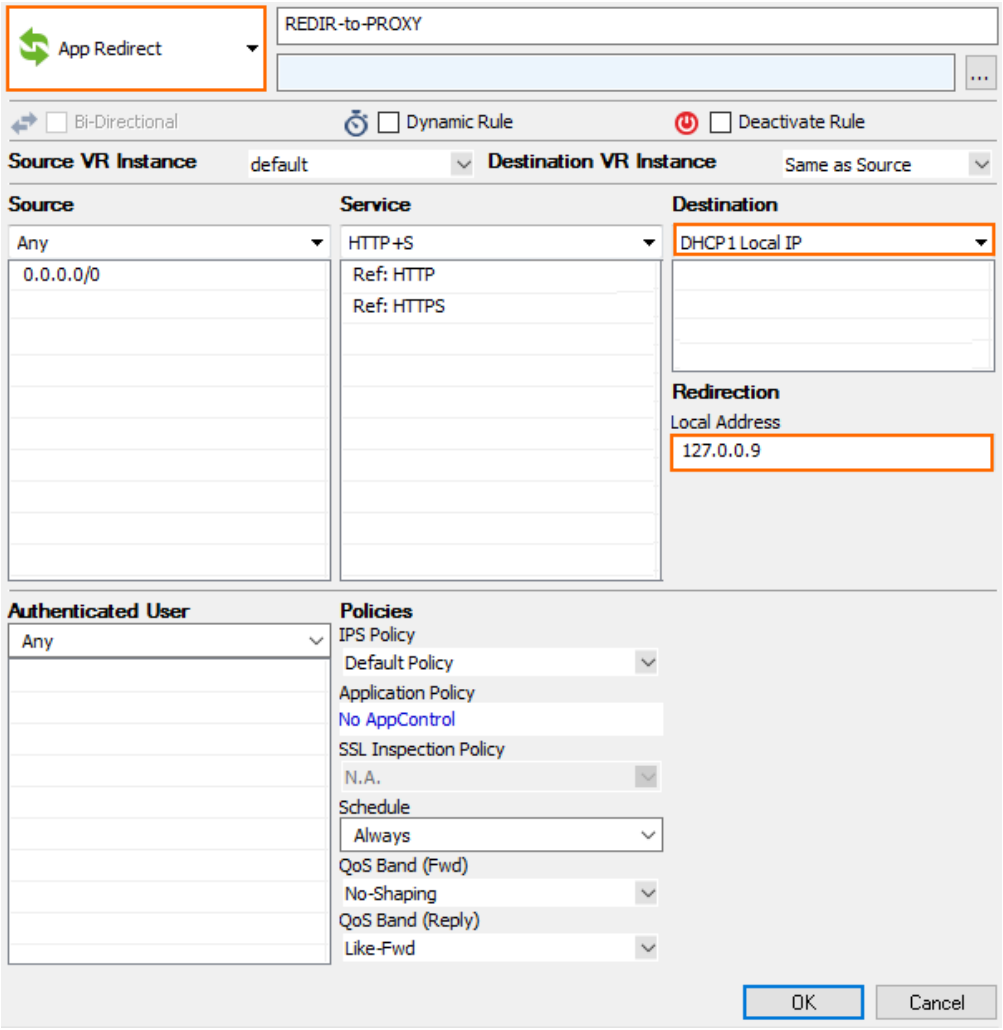
- **Custom external object 1** – internal IP address
- **Custom external object 2** – internal network address
- **Custom external object 3** – external IP address

For more information, see Custom External Network Objects.

Configuring Service Listeners and App Redirect Access Rules

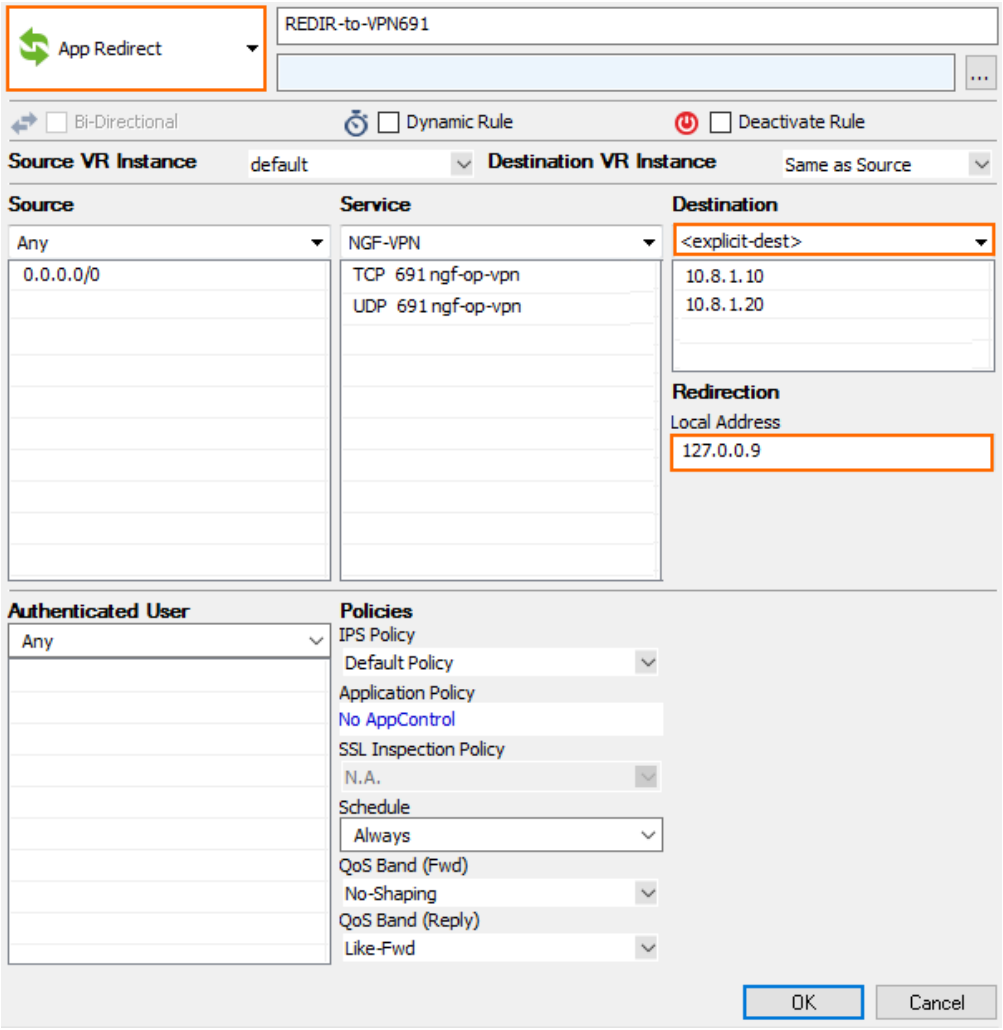
Stand-Alone Firewalls

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.



High Availability Clusters

High availability clusters must use static IP addresses as the management interface. Since floating IP addresses are not supported in the public cloud, 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.



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

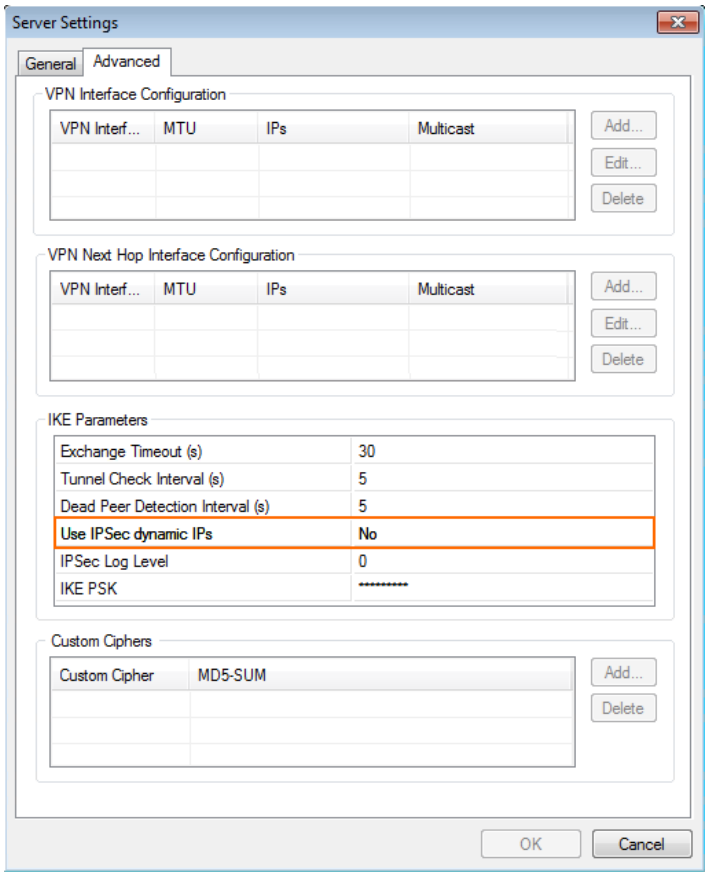
Configure an IKEv1 client-to-site or site-to-site IPsec VPN.

For more information, see Client-to-Site VPN or Site-to-Site VPN.

Step 2. Disable the IPsec Dynamic IP Setting

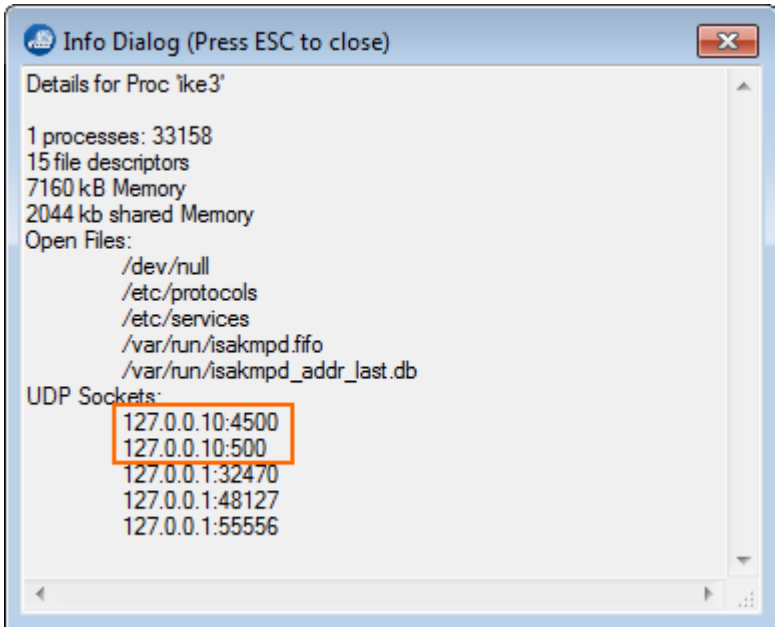
Open the **VPN Settings - Server Settings** and, in the **Advanced** tab, change **Use IPSec dynamic**

IPs to **No**. This disables the 0.0.0.0 listener for the ike3 (IPsec IKEv1) daemon.



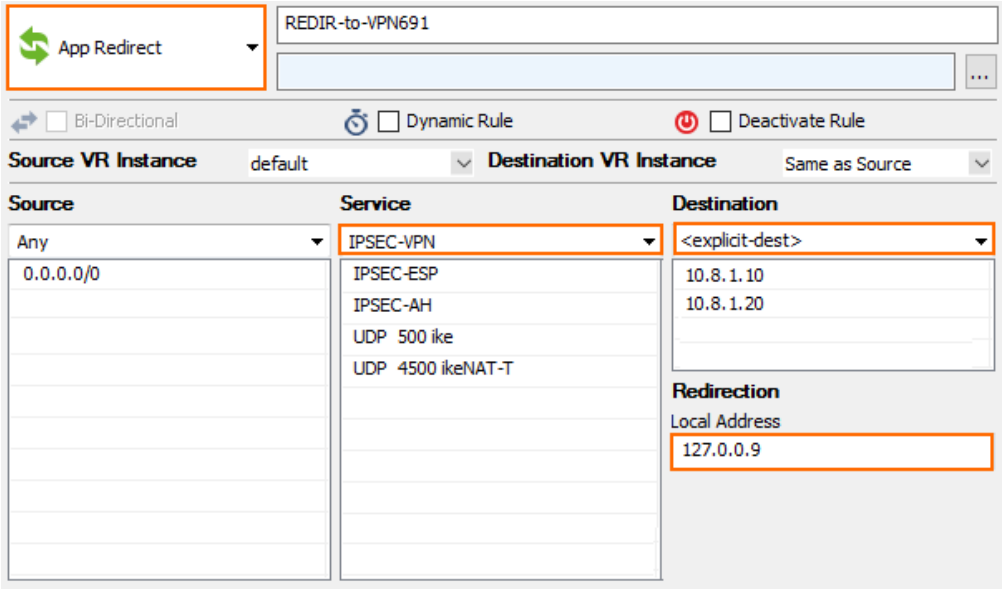
Step 3. Verify the ike3 Listeners

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.



Step 4. Create an 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.



Restoring a PAYG CloudGen Firewall 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 CloudGen Firewall.

Step 1. Create PAR File

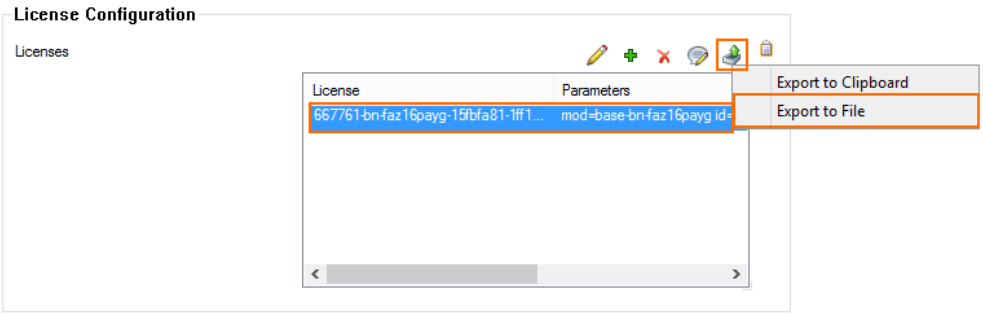
On the source PAYG CloudGen Firewall, create a PAR file.

For more information, see How to Back Up and Restore Firewall and Control Center Configurations or How to Create PAR or PCA Files on the Command Line.

Step 2. Export the PAYG License on a New Firewall VM

On the destination PAYG CloudGen Firewall, 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**.

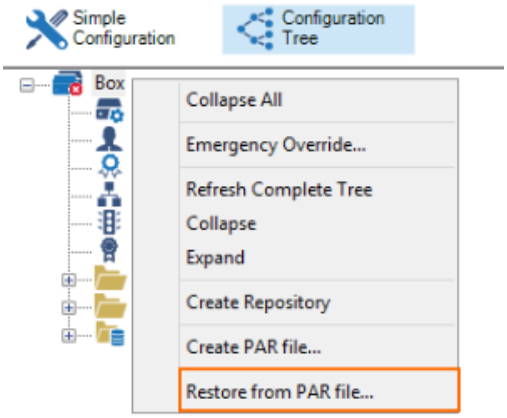


4. Save the lic file.
5. Click **Unlock**.

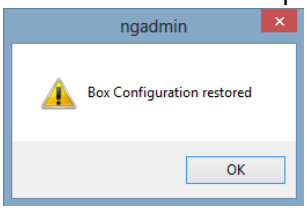
Step 3. Restore from the PAR File

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