Best Practice - Azure Public Cloud

https://campus.barracuda.com/doc/42043761/

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

In this article

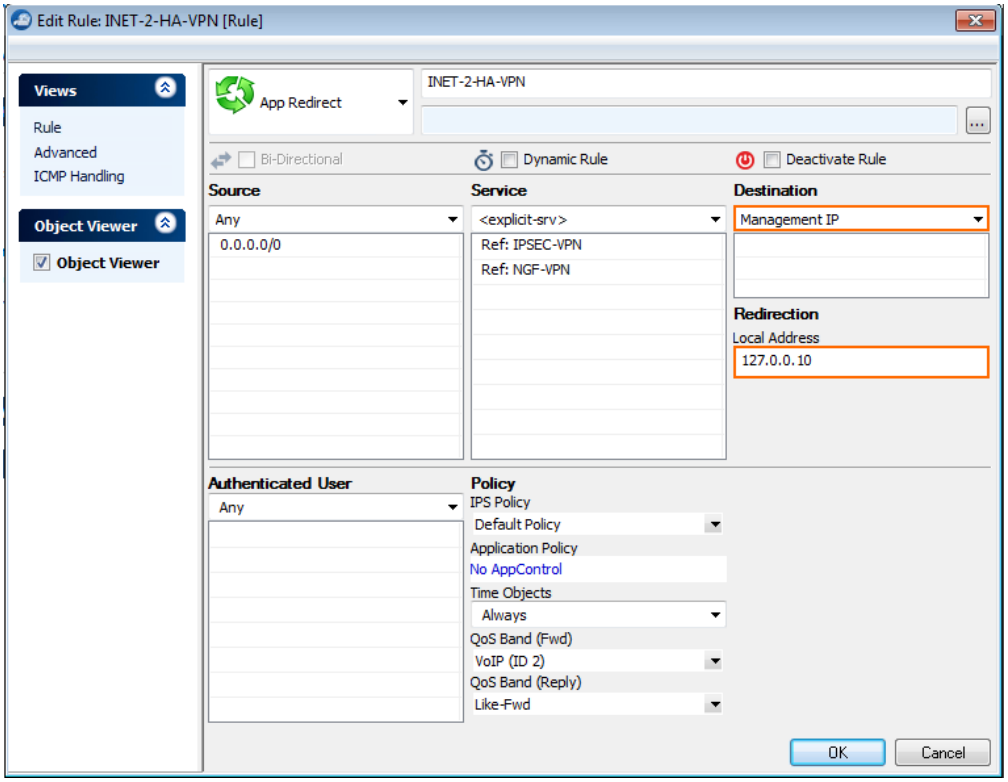
The Barracuda NG Firewall automatically fills the custom external network objects with network information acquired from the Azure Cloud:

- 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.

When using the Barracuda NG Firewall in an HA cluster, special consideration must be made for services running on the virtual server. Since both HA units use different IP addresses (which cannot be transferred to the other unit during failover), all services must listen on the loopback interface. You must also create app redirect access rules with the **Management IP** network object as the destination.

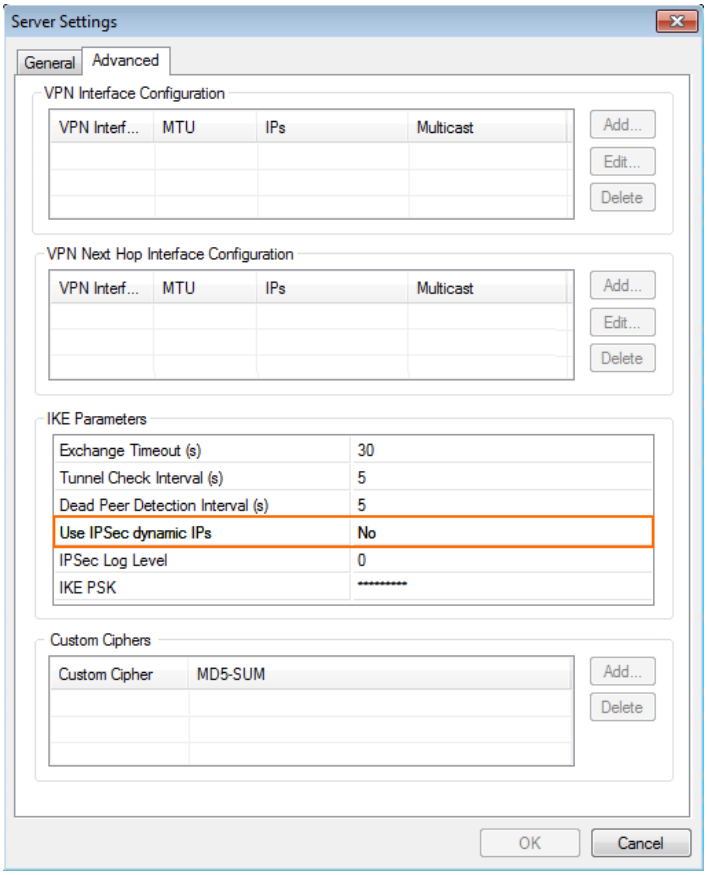
See below for an example app redirect access rule for a Barracuda NG Firewalls HA cluster.
Use **Any (**not **Internet)** as the source to also enable connections from other clients in the VNET:



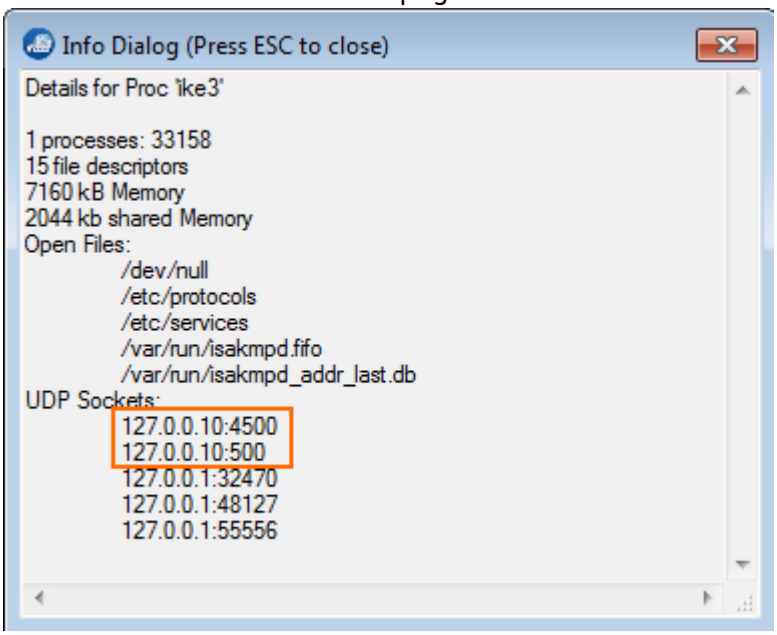
Configuring Client-to-Site IPsec VPN on the NG Firewall in an HA Cluster in Azure

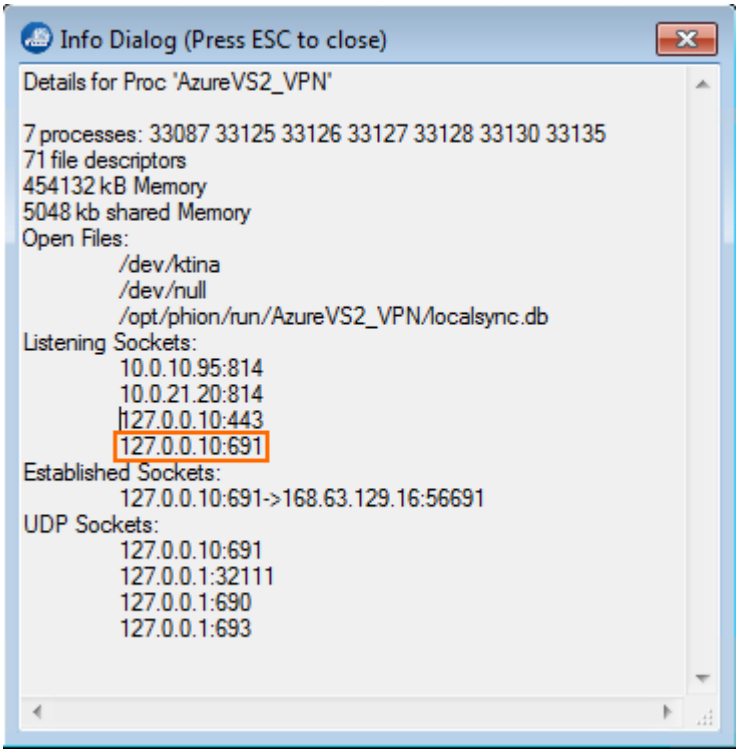
Configure the VPN service to listen on a 127.0.0.X address and create an app redirect access rule. Use **Any** as the source if you are using the Azure Connectivity Agent. Redirect both **IPsec-VPN** and **NGF-VPN** network objects to the VPN service because TCP port 691 is used by the Azure load balancer as the probing port. See Configuring Services on Barracuda NG Firewall HA clusters in Azure above for more information.

- Configure a Client-to-Site IPsec VPN (with or without PSK). For more information, see Client-to-Site VPN.
- Open the **VPN Settings - Server Settings** and, in the **Advanced** tab, change **Use IPSec dynamic IPs** to **No**.



- Verify that the **ike3** and **Tina VPN** processes are not listening on port TCP/691 or UDP/500/4500 on the management IP address. This is necessary to ensure that the traffic is handled by the Forwarding Firewall Service (and not the Host Firewall service). Open the **CONTROL > Resources** page and double-click on the **ike3** / **Tina VPN** process:





- IPsec VPN clients can only use one IP address for the destination. The VIP/RIP of the cloud service must be used to access the VPN service. Two Azure load balanced endpoints for **UDP 500** and **UDP 4500** (for ESPoUDP) must be created. Use **TCP Port 691** as the probing port and set the **probing interval** to the shortest possible setting: **5 seconds**.
- Add the two load balanced endpoints to both primary and secondary NG Firewalls.

The failover of the virtual server is almost instantaneous. The Azure load balancer, however, takes about 10 seconds to redirect traffic to the secondary unit. This may cause existing client-to-site connections to be interrupted. No traffic can be transmitted through the Client-to-Site VPN tunnel during the failover process.

Figures

1. BP_Azure01.png
2. BP_Azure02.png
3. BP_Azure03.png
4. BP_Azure04.png