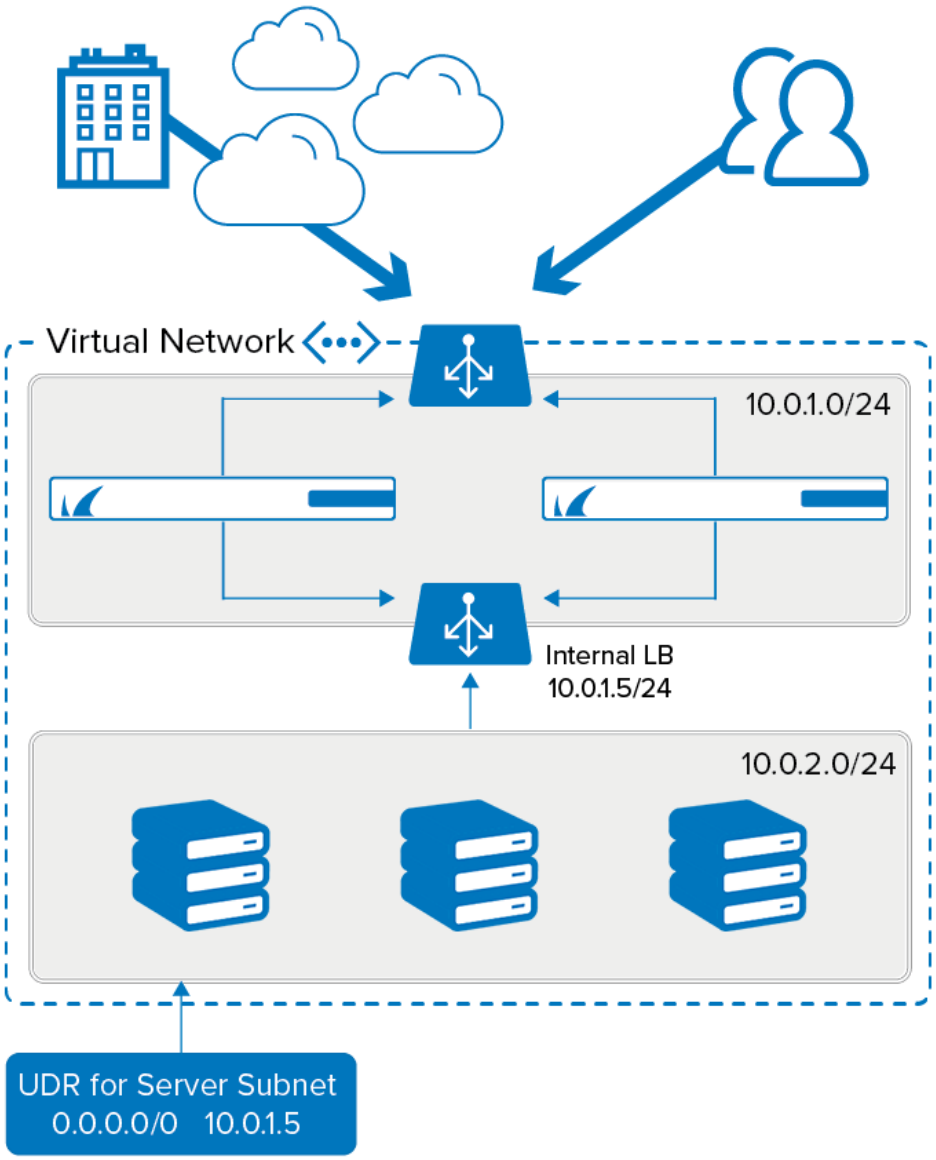
User Defined Routing in Azure

https://campus.barracuda.com/doc/98218387/

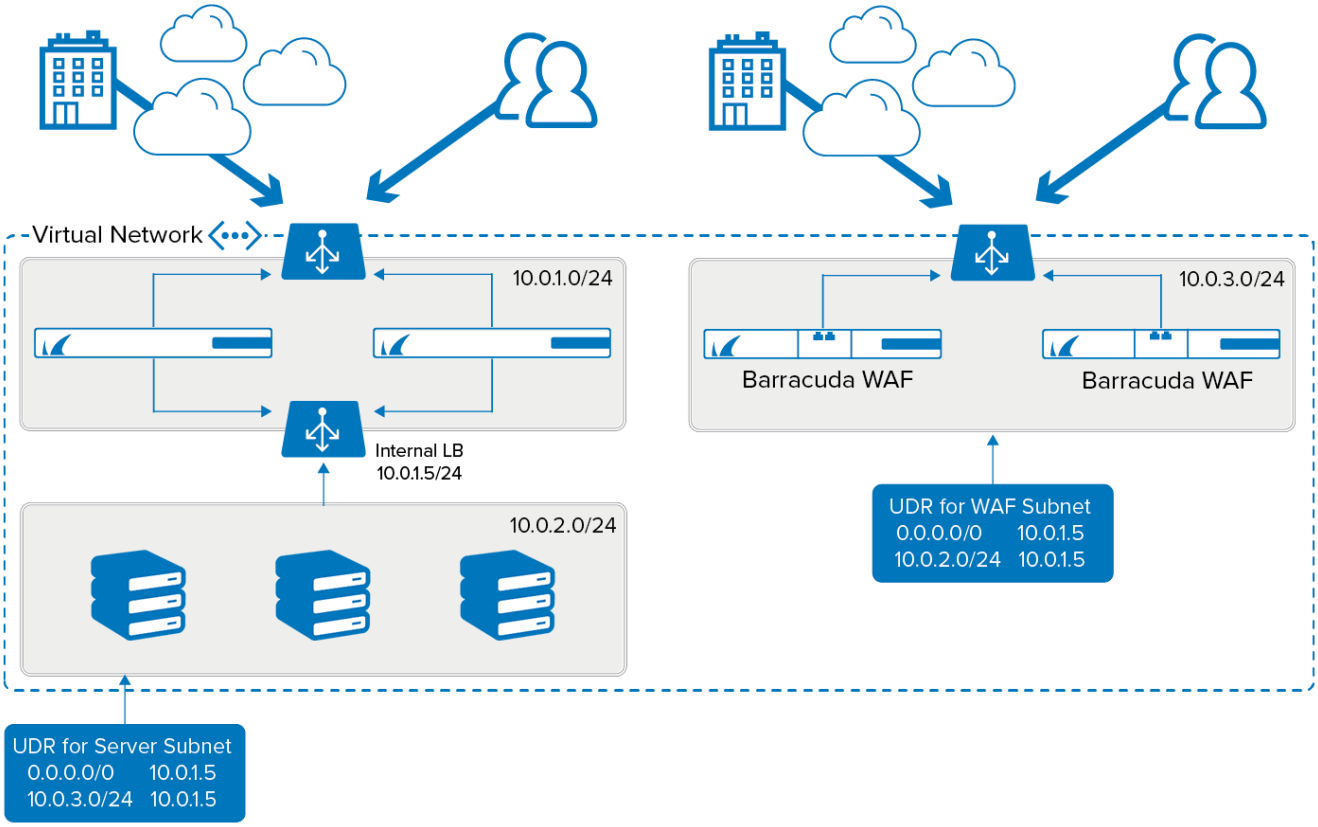
User Defined Routes (UDRs) can be used to override default routing in Azure. These routes are assessed by Azure using the longest prefix match algorithm. For example, a route table has two routes: One route specifies the 10.0.0.0/24 address prefix, while the other route specifies the 10.0.0.0/16 address prefix. Azure routes traffic destined for 10.0.0.5, to the next hop type specified in the route with the 10.0.0.0/24 address prefix, because 10.0.0.0/24 is a longer prefix than 10.0.0.0/16, even though 10.0.0.5 is within both address prefixes. Therefore, to route the traffic correctly to the virtual appliance, you must override the default, Azure provided routes with more specific routes back to the virtual appliance.

Example Routing Scenario: CloudGen Firewall HA Cluster



In the scenario above, the traffic arrives at the external load balancer in Azure, is forwarded on to the active CloudGen Firewall and then is forwarded on via the network interface of the active firewall. As the CloudGen Firewalls can route to all subnets in the VNet, the traffic arrives successfully at the servers in the server subnet. To avoid asynchronous routing, the traffic needs to return via the same CloudGen Firewall interface. So on the return journey, traffic leaving the server subnet must be routed via the internal load balancer, which will direct it to the active firewall interface. If the UDR routing all traffic back to the internal load balancer was not in place, the traffic would route out to the internet using the default routes provided by Azure, which would result in asynchronous routing, or a routing triangle, as the traffic would not be returning back the same way as it came.

Example Routing Scenario: CloudGen Firewall HA Cluster with WAF Cluster



In the above scenario, traffic to the WAF cluster in Azure is delivered via an external load balancer. As the WAF is a reverse proxy, the traffic from the WAF will always be from one of the internal IPs assigned to the WAF network interfaces. The UDR in the WAF subnet directs traffic to the spoke server traffic via the firewall ILB, which means all traffic destined for the web servers is inspected by the CloudGen Firewalls after it has passed through the WAFs. The CloudGen Firewalls then route the traffic from the active CloudGen Firewall instance to the web server. On the return journey, the traffic destined for the WAF is directed by UDR to the ILB, then routed through the active firewall instance back to the WAF. Again, this use of UDRs prevents asynchronous routing by ensuring that traffic leaves the destination subnet via the same route as it arrived there.

For detailed information on how to configure user Defined Routes in Azure, see:

- How to Configure Azure Route Tables (UDR) using Azure Portal and ARM
- How to Configure Azure Route Tables (UDR) using PowerShell and ARM

Additional Reference

- https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

Figures

1. az_ha_udr_01.png
2. az_ha_udr_02.png