High Availability Deployment

https://campus.barracuda.com/doc/39813139/

High availability is supported on the Barracuda SSL VPN 480 and above. Clustering two Barracuda SSL VPNs provides you with a high-availability, fault-tolerant environment that supports data redundancy and centralized policy management. After you configure one HA unit, configuration settings are synchronized across the cluster. You can cluster the Barracuda SSL VPN in two ways: simple high availability or high availability with a load balancer.

Simple high availability

If you configure two or more Barracuda SSL VPNs in a high availability setup without a load balancer, configurations are synced between the units but only one unit processes traffic. The secondary unit is passive and monitors the health of the primary unit. If the active system becomes unavailable, the secondary unit takes over automatically.

For more information, see How to Configure a High Availability Cluster.

High availability with a load balancer

If you want all clustered Barracuda SSL VPNs to process traffic, use a load balancer (such as the Barracuda Load Balancer) to direct traffic to the HA units while maintaining session persistence. You must have a load balancer to spread the load over all Barracuda SSL VPN cluster members. It is recommended that you configure the Barracuda Load Balancer in Bridge-Path (recommended) or Route-Path mode.

To cluster your Barracuda SSL VPNs with a load balancer, complete the following tasks:

1. Configure the Barracuda Load Balancer. For instructions, see Barracuda Load Balancer Bridge-Path Deployment or How to Set Up a Barracuda Load Balancer for Route-Path Deployment.
2. Configure Simple High Availability. See How to Configure a High Availability Cluster.