High Availability

https://campus.barracuda.com/doc/4259911/

Introduction

The **ADVANCED > High Availability** page allows you to cluster two Barracuda Web Application Firewalls in a high availability setup. Both units must be able to communicate with each other via their WAN ports. The Barracuda Web Application Firewall uses:

- TCP port 32575 to synchronize configuration between clustered units.
- TCP port 8002 to communicate with the peer unit.
- UDP port 32576 to exchange the Heartbeat in clustered units.

The Barracuda Web Application Firewall supports both Active-Standby and Active-Active configuration. In Active-Standby, one unit serves all requests for the Services in Vsite(s) configured while the other unit is in the Standby state. In Active-Active, both units serve requests for the Services in Vsite(s) that are configured to be active on individual units.

> The hardware devices and virtual machines should be of the same model and using the same firmware version while clustering. Note that:
>
> - Clustering a hardware appliance with a virtual machine or vice versa is not supported.
> - Clustering hardware appliances or virtual machines with different models is not supported.

Active-Active Setup

If different Vsites are active on each of the unit, and serving requests, the units are in Active-Active setup
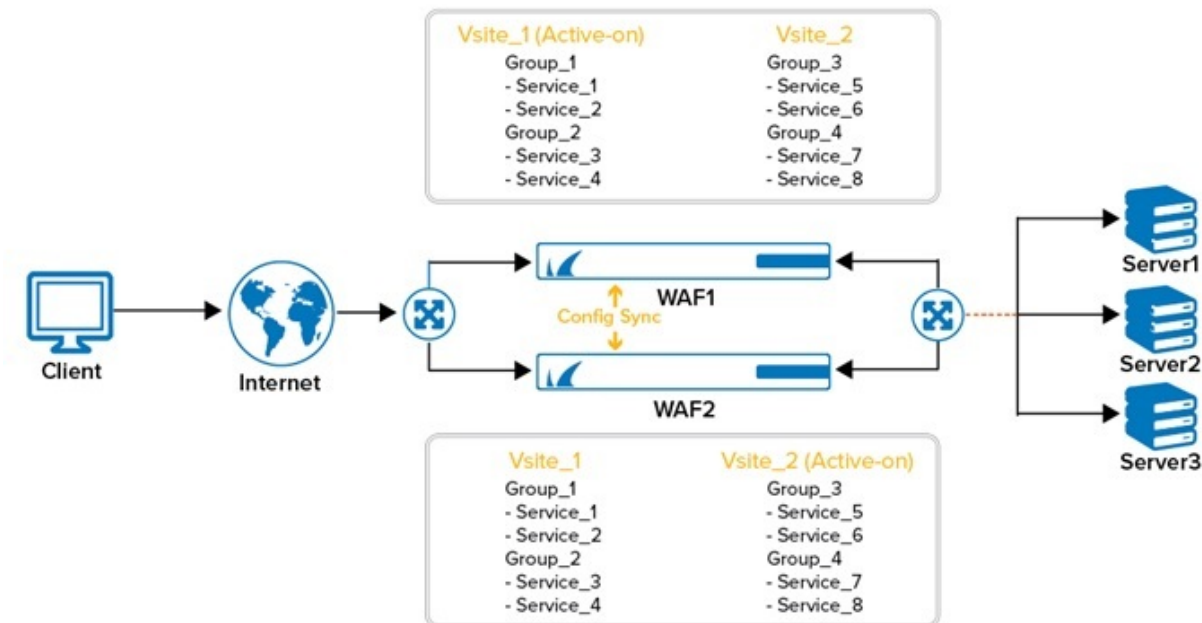
Active-Standby Setup

If all configured Vsites are active on one unit and the other unit is ready to handle traffic, the units are in Active-Standby setup.

A unit can be in Standby state in either of these two scenarios:

- If the administrator has configured all Vsite(s) to be active on one unit, and the other unit is ready to handle traffic.
- If the unit that was active and handling traffic had failed, restores from the Failed state and is ready to resume operation. This can occur only when the units are in **Manual** mode.S

From the beginning, for all WAF models, Active-Passive configuration is being supported. Active-Active configuration was introduced in version 7.7 and is available in the Barracuda Web Application Firewall *660* and above models. For information on High Availability in previous firmware versions, call Barracuda Networks Technical Support.

Each linked Barracuda Web Application Firewall sends a custom "heartbeat" to the other unit using UDP, providing continual status updates. If one of the units fails to send a heartbeat within nine (9) seconds, or sends a status indicating its state as "Failed", the Active unit assumes all active Services of the failed unit and continues to process traffic.

Each Barracuda Web Application Firewall to be added to a cluster must meet the following requirements:

- It must have a unique WAN IP address. The Barracuda Web Application Firewalls uses the WAN IP address for joining the units in cluster and configuration synchronization.
- It must have connectivity to (can ping successfully) the other appliance on the WAN interface.
- It must be co-located (WAN Interface) on the same switch (or physical network).

The "heartbeat" packets are sent through the WAN interface for determining the state of the Peer unit in HA by default. The **Advanced Cluster Settings** section on the **ADVANCED > High Availability** page provides the administrator an option to configure the interfaces (WAN, LAN or/and MGMT) on which the heartbeat packets needs to be sent. It also provides the flexibility to configure the frequency of heartbeat messages. The **Advanced Cluster Settings** is an advanced feature and is available only when **Advanced Settings** is set to *Yes* on the **ADVANCED > System Configuration** page.

It is recommended to send the heartbeat packets through multiple interfaces to reduce false positives.

When Barracuda Web Application Firewall devices are set up in clustered mode, Barracuda Networks recommend managing the systems through the device web interface.

To ensure proper routing from the back-end servers in case of failover:

- Add a virtual IP address on the LAN interface from the **NETWORKS > Interfaces** page.
- Use this virtual IP address as the routing address for WAN traffic on the real server routing tables (or to the intermediate router's routing tables if the server is in a different subnet).

Do not use the LAN IP address for routing in a HA setup as it is not synchronized or failed over in a cluster.

Figures

1. HAimg1.jpg