# How to Set Up a High Availability Environment with Two Barracuda Web Application Firewalls

https://campus.barracuda.com/doc/4259898/

The **ADVANCED > High Availability** feature enables you to cluster two Barracuda Web Application Firewalls as an Active-Standby or Active-Active pair. In an Active-Standby setup, one unit serves all requests for the services in configured Vsite(s), and the other unit is ready to handle the traffic. In an Active-Active setup, both units serve requests for only the services in Vsite(s) configured on the respective unit.

## Cluster Two Barracuda Web Application Firewalls

1. For each system follow the instructions in Step 1: Installing the Barracuda Web Application Firewall. Each Barracuda Web Application Firewall in a cluster must have the same firmware version installed.
2. Ensure each system has the following basic configuration settings:
    - Unique WAN IP address, LAN IP address, and Default Host Name on the **BASIC > IP Configuration** page.
    - The DNS server IP address may be unique for each or the same on both systems.
    - If both systems in the cluster are in the same network, ensure they are set to the same time and time zone on the **BASIC > Administration** page. This prevents configuration synchronization issues.
3. From the **ADVANCED > Task Manager** page on the Barracuda Web Application Firewall 1, verify that no processes are running. Do the same for Barracuda Web Application Firewall 2. No processes should be running on either appliance when you join systems together.
4. Always initiate the **Join Cluster** operation from the unit that needs to inherit the configuration. The unit from which the join cluster is initiated will have its configuration overwritten. To ensure that the backup unit has no previous configuration settings, invoke **Clear Configuration** from the **ADVANCED > Troubleshooting** page to restore the unit to its initial configuration.
5. From the **ADVANCED > High Availability** page on the Barracuda Web Application Firewall 1, enter the **Cluster Shared Secret.** As a best practice, use a unique account for this integration point and grant it the least level of privileges required, coordinating with the administrator. This account requires READ privileges. For additional information, see Security for Integrating with Other Systems - Best Practices.

    **Cluster Shared Secret** can include alphanumeric characters, periods (.), hyphens (-) and underscores (_). Any other special characters such as space, semicolon, asterisk, etc., are not allowed.
6. Click **Save Changes**.
7. From the **ADVANCED > High Availability** page on the Barracuda Web Application Firewall 2, do the following:
    1. Enter the same **Cluster Shared Secret**, and click **Save Changes**. Both units in a cluster must have the same Cluster Shared Secret to communicate with each other.

    2. In the **Clustered Systems** section, enter the WAN IP address of the Barracuda Web Application Firewall 1, and click **Join Cluster**. Never cancel a Join Cluster in progress. The unit from which the Join Cluster is executed becomes the designated backup unit. That is, Barracuda Web Application Firewall 1 becomes Primary and Barracuda Web Application Firewall 2 becomes Backup.
8. On each Barracuda Web Application Firewall, refresh the **ADVANCED > High Availability** page, and verify the following:
    1. Each system's WAN IP address appears in the Clustered Systems list.
    2. The status is green for both units. This indicates the communication status. See Status Indicators.
9. The High Availability status can be viewed on the **BASIC > Dashboard** page, under **Performance Statistics**. This shows the role and state of each unit. You can also view the High Availability status for 2 nodes when the nodes are in Active/Passive status and the cluster Status for all the nodes when the nodes are in Active-Active status. To see the status of the unit, mouse over host name and the icons.

**Clustering in Bridge Mode**

- To cluster two machines in Bridge mode for High Availability, first put the desired secondary or backup unit in proxy mode. After you join the two using the above steps, the secondary machine will synchronize its configuration to the primary and revert to Bridge mode.
- Note that on the **BASIC > IP Configuration** page, the options **Bypass on Failure** and **Hard Bypass** should be set to *No* in order to cluster two units.

In Proxy mode, if **Client Impersonation** is enabled,do the following:

1. Create a virtual interface on the port that is used to connect to the backend servers.
2. Configure the IP address of the virtual interface as the default gateway on the servers.

#### Status Indicators

The status of clustered units:

- (✓) **Active**/**Standby** state – The unit is up and serving incoming service requests (if any), OR the unit is up and ready to assume services (if any).
- (✗) **Failed** state – The unit is down due to any of the reasons below:
    1. **Link Down** – If **Monitor Link** for WAN, LAN or Management is selected in the **ADVANCED > High Availability** page, and the corresponding link is down, the system goes into a Failed state.
    2. **Inability to Serve Traffic** – Instability in any traffic processing module that prevents it from serving traffic will cause the system to go into a Failed state.
    3. **Lost Heartbeat** – When the backup unit has not received a heartbeat from the primary unit for 9 seconds, it concludes that the primary unit is down or dead, and it executes failover.

- (▲) **Initializing** state – The unit is in initializing state, that is, the JOIN CLUSTER operation is running.

When Barracuda Web Application Firewall devices are set up in clustered mode, Barracuda Networks recommends managing the systems through the device web interface. Performance is degraded when managing clustered systems through Barracuda Appliance Control.

## Multiport

Multiport Barracuda Web Application Firewall supports heterogeneous and homogeneous clustering. If the cluster is performed between two units with the same model but different number of ports, the cluster is known as a heterogeneous cluster. When the units of same model and ports are clustered, it is known as a homogeneous cluster.

The Barracuda Web Application Firewall provides the following models with different number of ports:

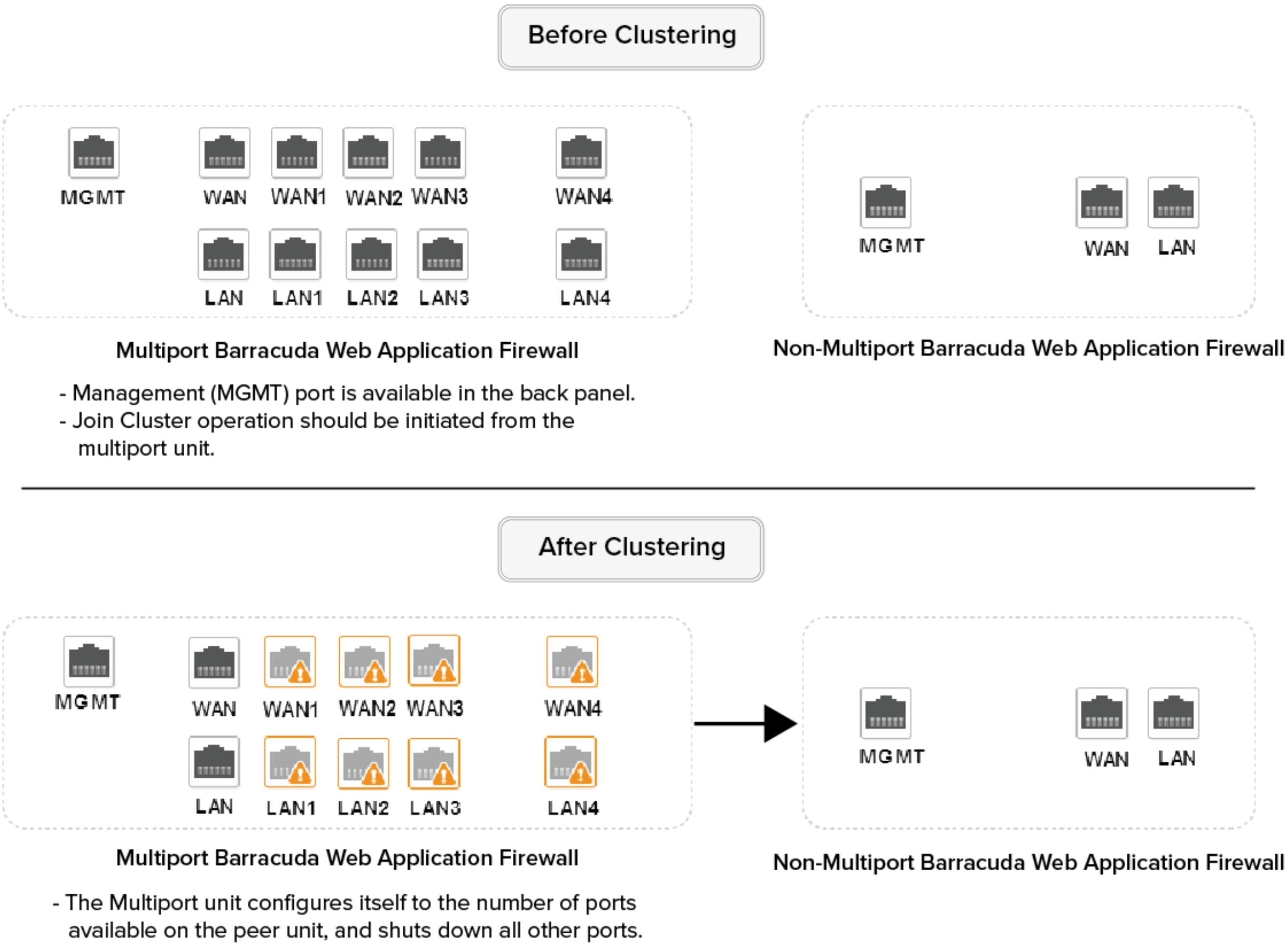
| **The Barracuda Web Application Firewall Model Numbers** | **Ethernet Ports** |
|---|---|
| 860 | 8 x 1 GbE CU without bypass |
| 861 | 8 x 1 GbE CU with bypass |
| 862 | 8 x 1 GbE SFP (Fiber) with bypass |
| 960 | 8 x 1 GbE CU + 2 x 10 GbE CU without bypass |
| 961 | 8 x 1 GbE CU + 2 x 10 GbE CU with bypass |
| 963 | 2 x 1 GbE CU without bypass |
| 964 | 8 x 1 GbE + 2 x 10 GbE SFP (Fiber) with bypass |

#### Heterogeneous Clustering

In the heterogeneous scenario, you can cluster two units with same model but different number of ports. For example, a multiport Barracuda Web Application Firewall 860 can be clustered with a non-multiport Barracuda Web Application Firewall 860. In this case, the **Join Cluster** operation should be initiated from the multiport unit, that is, multiport Barracuda Web Application Firewall 860.

After the cluster, the multiport Barracuda Web Application Firewall configures itself to the number of ports available on the peer unit and shuts down all other ports on the unit. For example, consider multiport Barracuda Web Application Firewall 860 as WAF1 and non-multiport Barracuda Web Application Firewall 860 as WAF2, where WAF1 has 11 ports and WAF2 has 3 ports. The **Join Cluster** operation is initiated from WAF1. After the cluster, WAF1 keeps 3 ports open out of 11 ports, and shuts down the remaining 8 ports.

It is NOT recommended to do any configuration change when the Barracuda Web Application Firewall units are in HA and running with different firmware versions.


Before Clustering
MGMT
WAN
WAN1
WAN2
WAN3
WAN4
LAN
LAN1
LAN2
LAN3
LAN4
Multiport Barracuda Web Application Firewall
- Management (MGMT) port is available in the back panel.
- Join Cluster operation should be initiated from the multiport unit.
MGMT
WAN
LAN
Non-Multiport Barracuda Web Application Firewall
After Clustering
Multiport Barracuda Web Application Firewall
- The Multiport unit configures itself to the number of ports available on the peer unit, and shuts down all other ports.
Non-Multiport Barracuda Web Application Firewall

## Homogeneous Clustering

In the homogeneous cluster,

- The units with same model and ports are clustered.
- The units with homogeneous vx_aa_ha mode are allowed to join cluster.

For more information on clustering, refer to the High Availability article.

In multiport HA, servers reachable via LAN1/LAN2/LAN3/LAN4 will always remain down on the secondary/backup unit. This is because the custom virtual interface IP addresses are not configured on the secondary unit. Therefore, the backend servers are not reachable from the secondary unit. [BNWF-24346]

**Related Articles**

- Failover and Failback in an Active-Active Cluster
- How to Remove or Replace Units in a Cluster
- Updating the Firmware in Clustered Units

## Figures