How to Configure a High Availability Cluster

https://campus.barracuda.com/doc/39815181/

Follow these instructions to cluster your Barracuda SSL VPN systems. These instructions apply to both simple High Availability and for clustering with a load balancer. In order to guarantee unobstructed synchronization flow, Barracuda Networks strongly recommends not to use more than two appliances per cluster.

Simple high availability

Simple High Availability (HA) can be used in cases where more than one Barracuda SSL VPN is available to create a failover cluster but a load balancer is not in use. Only one SSL VPN system will actively process traffic. The other system(s) will act as passive backup(s). In an HA cluster, a virtual IP address is used to access the SSL VPN service. If the active system becomes unavailable, one of the passive systems in the cluster will become active and serve requests directed to the virtual IP address. You will use the individual IP addresses of the systems in the cluster for management. When the originally active SSL VPN appliance becomes available again, it will act as a passive backup.

Before you begin

- Make sure that each Barracuda SSL VPN has the same model and firmware version. It is possible to mix hardware and virtual appliances. To check the firmware version, log into the appliance interface using the **admin** account, and go to **ADVANCED > Firmware Update**.
- Make sure that each Barracuda SSL VPN has the same time zone configured on the **BASIC > Administration** page.

Step 1. Prepare the Barracuda SSL VPN systems for clustering

Step 1a. Create a backup

Create a backup of the existing Barracuda SSL VPN configuration on each system that should be in the cluster.

1. Log into the appliance interface using the **admin** account.
2. Go to **ADVANCED > Backup.**
3. Create a backup of the existing Barracuda SSL VPN configuration.
4. After the backup is created, go to **ADVANCED > Task Manager** and verify that no processes are running.

Step 1b. Enable SSLv2

Clustering of SSL VPN units requires the SSLv2Hello protocol. To enable SSLv2, perform the following steps on each system that will be in the cluster:

1. Log into the SSL VPN web interface using the **ssladmin** account.
2. Go to **ADVANCED > Configuration**.
3. In the **Cryptography** section, select **SSLv2Hello** from the **Supported Protocols** list.
4. Click **Add** to add it to the **Selected Protocols** list.
5. Click **Save Changes**.

Step 2. Create a high availability cluster

To create a simple high availability cluster:

1. Log into the appliance interface using the **admin** account.
2. Go to **ADVANCED > Linked Management**.
3. In the **Cluster Settings** section, enter the **Cluster Shared Secret**. This is the password shared by all Barracuda SSL VPN appliances in this cluster. It is limited to only ASCII characters.
4. Click **Save Changes**.
5. In the **Add System** field in the **Clustered Systems** section, enter the IP address of a system in the cluster (or, the first system if the cluster has not yet been created). A fully qualified domain name can be entered, but could cause name resolution issues. so is not recommended.
6. Click **Join Cluster**. The time to complete the join depends on the number of users, domains, and the load on each Barracuda SSL VPN appliance. During this time, the configuration from the other system will be copied onto this system. The system will restart, and you will need to log in and navigate to this page.
7. In the **Simple High Availability** section, enter the Virtual IP address.
8. Click **Save Changes**.

Step 3. Verify the cluster status

On each system in the cluster, perform the following:

1. Log into the appliance interface using the admin account.
2. Go to **ADVANCED > Linked Management**.
3. Refresh the **ADVANCED > Linked Management** page to view the updated status.
4. Verify that the **Clustered Systems** list contains the IP address of each clustered system.
5. Verify that the **Connection Status** indicates that each clustered system is up and communicating with this system. The column displays green for each system that is available and red for each system that cannot be reached. Initially, it may take up to a minute for the

status light to turn green.
    - The **Synchronization Latency** field tells how long it takes to send updates to each of the other systems in the cluster. The value of this field should be 2 seconds or less. If it is greater, configuration changes may not be propagated correctly.
    - The **Mode** column in the **Clustered Systems** table should usually show all systems in the cluster as being **Active**. If a system is in standby mode, changes to its configuration are not propagated to other systems in the cluster.
6. On the first, initially active system, select the **High Availability Master** option.

Adding appliances to a cluster

Any Barracuda SSL VPN appliance that is added to the cluster will have most of its local data (except user data and that specified in **Non-Clustered Data**) overwritten with settings extracted from the cluster. The first system (the one identified first in the Add System field) is the source for the initial settings.

1. Log into the appliance interface using the **admin** account.
2. Go to **ADVANCED > Linked Management**.
3. In the **Add System** field in the **Clustered Systems** section, complete steps 4 and 5 as described in the **Create a High Availability Cluster** task above.
4. (Optional) Distribute the incoming SSL traffic to each Barracuda SSL VPN using a load balancer.

Non-clustered data

Energize updates do not synchronize across systems in a cluster.

The following data is not propagated to each system in the cluster:

- **IP Address**, **Subnet Mask**, and **Default Gateway** (on the **BASIC > IP Configuration** page).
- **Primary DNS Server** and **Secondary DNS Server** (on the **BASIC > IP Configuration** page).
- Serial number (this will never change).
- **Hostname** (on the **BASIC > IP Configuration** page).
- All SSL information, including saved certificates (on the **BASIC > SSL Certificate** page).
- Any advanced IP configuration (models 600 and above, on the **ADVANCED > Advanced Networking** page).
- Administrator password.
- **Cluster Shared Secret**, though this must be the same for the cluster to work properly (on the **ADVANCED > Linked Management** page).
- **Time Zone** (on the **BASIC > Administration** page).
- The appliance GUI and SSL VPN HTTP and HTTPS ports.
- Whether the latest release notes have been read.
- All customized branding (models 600 and above, on the **ADVANCED > Appearance** page).