

Clustering two or more Barracuda SSL VPNs together provides you with a high availability, fault-tolerant environment that supports data redundancy and centralized policy management. Easily scalable simply by linking in additional devices, clustered Barracuda SSL VPNs are also easy to configure -- once you configure one of the devices, configuration settings are synchronized across the cluster almost immediately. Clustering for High Availability is available on the Barracuda SSL VPN 480 and higher.

The two main steps for deploying clustered Barracuda SSL VPNs are **configuring a Load Balancer** (recommended), and **configuring the Barracuda SSL VPN cluster**.

Configuring the Barracuda Load Balancer

It is not required to have a load balancer to implement clustering, but it is highly recommended that you have a load balancing solution in place because the Barracuda SSL VPN itself does not load balance between clustered nodes. The steps here describe how to configure the Barracuda Load Balancer to work in front of clustered Barracuda SSL VPNs.

Lay out your network

It is best to install the Barracuda SSL VPNs on a separate network segment so that the only connection to the rest of the LAN is via the LAN port of the Barracuda Load Balancer. The LAN port connects to the same segment that the Barracuda SSL VPNs are on, while the WAN port connects to the rest of the LAN. In addition to the IP addresses of each Barracuda SSL VPN and of the Barracuda Load Balancer itself, you will also need a separate IP address that will be used as the Virtual IP by the Barracuda Load Balancer, to balance the incoming connections for the Barracuda SSL VPNs. Outbound traffic from your Barracuda SSL VPNs will go through the Barracuda Load Balancer via the network bridge.

Configure the VPNs on private IPs

The Barracuda Load Balancer should be configured as a Layer 4 device that terminates the SSL connections and forwards the HTTP traffic to the Barracuda SSL VPNs. Both Bridge-Path and Route-Path modes will work, but the easier method to configure is Bridge-Path.

To set up Bridge-Path on the Barracuda Load Balancer:

1. Log in as "admin" and go to the **BASIC > IP Configuration** page.
2. Check the "Operating Mode" section -- if it is not already set to Bridge-Path, click "Convert" to change the operation from Route-Path to Bridge-Path, and reboot.

Configure the Barracuda Load Balancer to have a Virtual IP address (VIP) that points to your pool of SSL VPNs. The WAN side of the Barracuda Load Balancer will have two IP addresses we need to consider: the Barracuda Load Balancer system IP address and the VIP that the cluster will use.

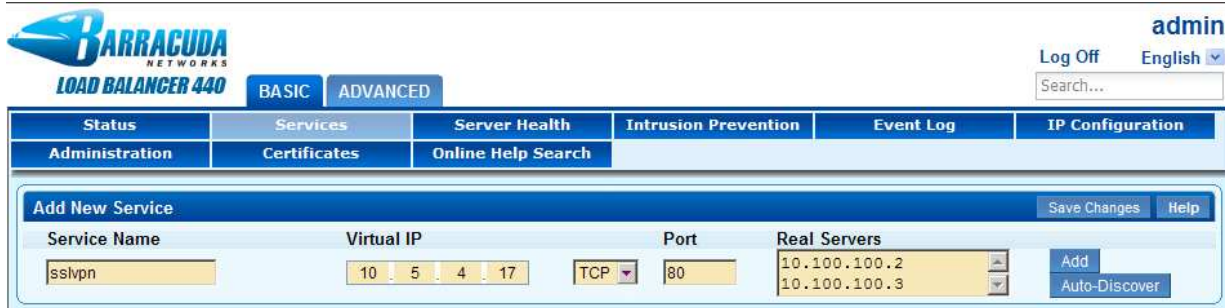
For example:

Network	Barracuda Load Balancer WAN Port	IP Address	Notes
10.5.0.0/17	System IP	10.5.16.8	The primary system IP address, used to configure the Barracuda Load Balancer.
10.5.0.0/17	Virtual IP	10.5.4.17	The Virtual IP that points to the cluster.

Once the Barracuda SSL VPNs are configured with their IP addresses and the Barracuda Load Balancer is configured with its WAN management and virtual IP addresses, it's time to configure the Virtual IP in the Barracuda Load Balancer.

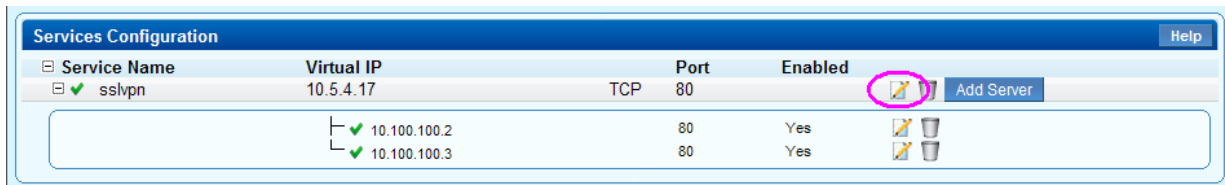
To configure the VIP on the Barracuda Load Balancer:

1. Navigate to **BASIC > Services** and add a new Service, using the IP address of the actual Barracuda SSL VPN servers on port 80 as shown below:



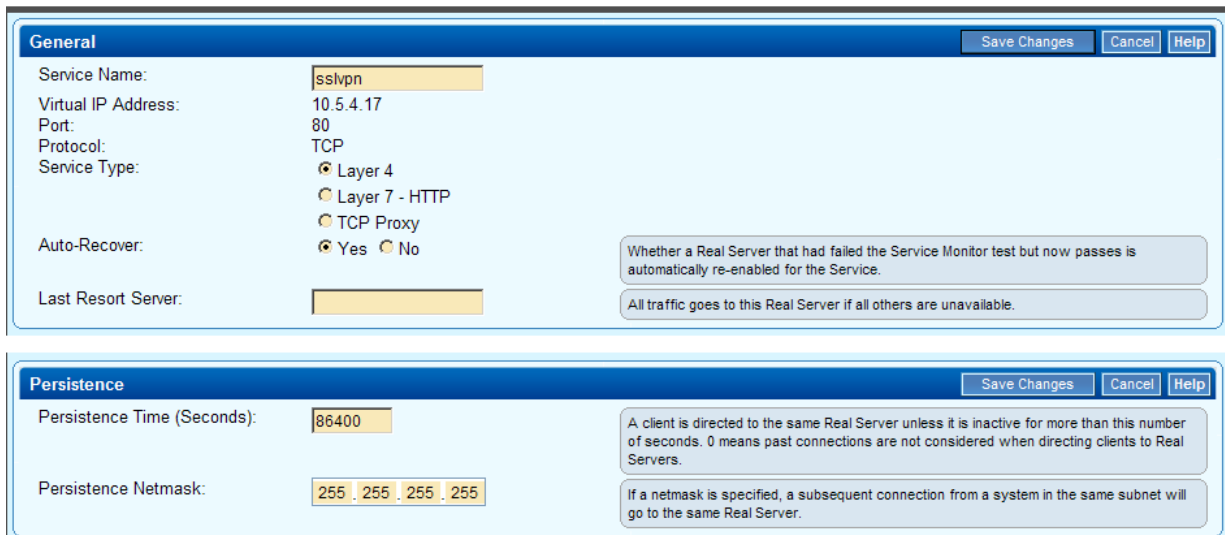
The screenshot shows the 'Add New Service' configuration page in the Barracuda Load Balancer 440 interface. The user is logged in as 'admin'. The interface includes a search bar and navigation tabs for 'BASIC' and 'ADVANCED'. The main configuration area is divided into sections: 'Status', 'Services', 'Server Health', 'Intrusion Prevention', 'Event Log', and 'IP Configuration'. The 'Services' section is active, showing a table with columns for 'Service Name', 'Virtual IP', 'Port', and 'Real Servers'. A new service named 'sslvpn' is being added with a Virtual IP of 10.5.4.17, Protocol of TCP, and Port of 80. The Real Servers are listed as 10.100.100.2 and 10.100.100.3. Buttons for 'Save Changes', 'Help', 'Add', and 'Auto-Discover' are visible.

2. Edit the Virtual IP service entry.



The screenshot shows the 'Services Configuration' page. It displays a table of services. The 'sslvpn' service is selected, and its configuration is shown below the table. The table has columns for 'Service Name', 'Virtual IP', 'Port', 'Enabled', and 'Add Server'. The 'sslvpn' service has a Virtual IP of 10.5.4.17, Port of 80, and is enabled. Below the table, the real servers are listed: 10.100.100.2 and 10.100.100.3, both with Port 80 and Enabled status. A pink circle highlights the edit icon for the 'sslvpn' service entry.

3. From this page, provide the SSL termination and determine session persistence. In this example Layer 4 (Client IP) persistence is used and the persistence timeout value is set for one day.



The screenshot shows the configuration pages for the 'sslvpn' service. The 'General' page is visible, showing fields for 'Service Name' (sslvpn), 'Virtual IP Address' (10.5.4.17), 'Port' (80), 'Protocol' (TCP), and 'Service Type' (Layer 4). The 'Auto-Recover' option is set to 'Yes'. The 'Last Resort Server' field is empty. The 'Persistence' page is also visible, showing 'Persistence Time (Seconds)' set to 86400 and 'Persistence Netmask' set to 255.255.255.255. Both pages have 'Save Changes', 'Cancel', and 'Help' buttons.

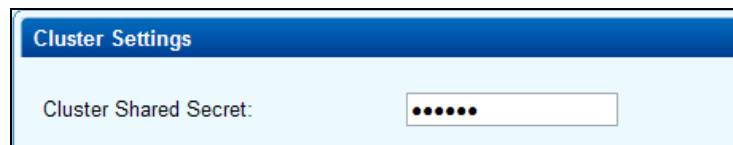
Configuring the Barracuda SSL VPNs

Prior to clustering your Barracuda SSL VPNs, make sure you do the following:

- **Create a backup** of your existing Barracuda SSL VPN configuration. This is to ensure that your configurations are not lost in case something goes wrong.
- Ensure all Barracuda SSL VPNs are **running the same firmware version**. If they are not, upgrade your systems to the latest firmware prior to clustering.


To cluster your Barracuda SSL VPNs:

1. Log into the Web interface at <http://<server>:8000> (or port 8443 if you are using SSL).
2. From the **ADVANCED > Linked Management** page, set your Cluster Shared Secret. Every Barracuda SSL VPN in the cluster must be configured with the same Shared Secret for them to be able to link with each other



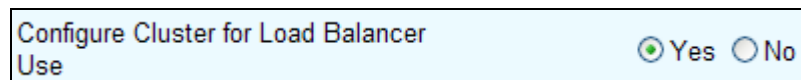
The screenshot shows a web interface titled "Cluster Settings". Below the title, there is a label "Cluster Shared Secret:" followed by a text input field containing six dots, representing a masked password.

3. Upon saving, the Barracuda SSL VPN will automatically restart.
4. After reboot, return to the **ADVANCED > Linked Management** page and in the Clustered Systems section, add the IP addresses of all Barracuda SSL VPNs that are to be a part of the cluster.



The screenshot shows a web interface with the text "Add a system to the cluster:" followed by a text input field and a blue button labeled "Join Cluster".

5. If you intend to use SSL offloading, then in the Barracuda Load Balancer Integration section select **Yes**. *Do not enable this option if you are using L4 session affinity with SSL handled by the end points.*



The screenshot shows a web interface with the text "Configure Cluster for Load Balancer Use" and two radio buttons: "Yes" (which is selected) and "No".

Note that you will only get a performance benefit from using SSL offloading if the Barracuda Load Balancer unit is more powerful than both Barracuda SSL VPN units combined (e.g., it is not worth offloading when using a Barracuda Load Balancer 330 with Barracuda SSL VPN 380s).

6. Refresh the page to get a list of all clustered nodes with their statuses in the Clustered Systems section -- a green light denotes a successful connection. If not all systems are showing a green light, wait a minute or two for the clustering process to complete then refresh the page again.

Setting non-proxied hosts

If the Barracuda SSL VPNs are using a proxy (**BASIC > IP Configuration**), then you must also configure non-proxy hosts in the Barracuda SSL VPN interface on port 443. To do this, log onto the Barracuda SSL VPN interface on all servers and from the **ADVANCED > Configuration > Proxies** page, make sure there is a non-proxied host entry for your IP range that the clustered servers are on (e.g. 192.168.0.*). Without this setting, data synchronization may not occur and your systems will not be truly clustered.