Clustering for High Availability
Barracuda Spam Firewall

This document describes the Clustering features of the Barracuda Spam Firewall 400 and 600. The clustering option will provide high availability in those environments that require it.

If you have any questions after reading this document, please contact Barracuda Technical Support at 408-342-5400 or email us at support@barracudanetworks.com. We also recommend that you check the Barracuda Networks User Forum at http://forum@barracudanetworks.com.

Barracuda Spam Firewall Version 3.X Clustering

Barracuda Networks has released an enhanced clustering option for the Barracuda Spam Firewall 400 and 600. True "Active/Active" clustering is now supported and provides robust and efficient data syncing for all Barracuda Spam Firewalls in the cluster. You can also now administer a cluster from a single Barracuda Spam Firewall user interface, even with up to eight Barracuda Spam Firewalls clustered on a LAN or WAN.

Barracuda Spam Firewalls can be easily added to or removed from the cluster with no loss of permanent data. Although you can also mix Barracuda Spam Firewall 400 and 600 models in a clustered environment, this is not recommended.

The following information is maintained by the clustered Barracuda Spam Firewalls:

- **System Configuration Information:** This information, except for IP address, is synchronized between all of the clustered Barracuda Spam Firewalls. A change to one of the clustered systems will be propagated to all of the other Barracuda Spam Firewalls.
- **User Account Settings and Configurations:** This information is synchronized between all of the clustered Barracuda Spam Firewalls. A change to one of the clustered systems will be propagated to all of the other Barracuda Spam Firewalls.
- **Message Logs:** Message logs from all of the clustered systems are viewable from any of the User Interfaces. However, the data resides on each Barracuda Spam Firewall separately. To safely backup these files it is suggested that users use the Syslog feature to capture all the data.
- **Bayesian Database:** This database is shared between all of the clustered systems.
- **Per User Quarantine Areas:** Per User Quarantine storage is synchronized between two of the clustered systems although the entire Per User Quarantine can be viewed from any system in the cluster. The actual emails reside on two machines within the cluster; one is the primary and the other is the backup.

This Barracuda Clustering functionality makes full redundancy and high availability easier to manage and more effective. Individual Barracuda Spam Firewalls can be added to, and removed from the cluster easily, and all of the necessary shared information is restored automatically. Of course, the removal of a system from the cluster will impact the capacity and performance of the cluster, but there is no loss of permanent data.

Load Balancing and Failover

How failover is handled depends on the load balancing strategy implemented. If you use MX records to load balance multiple Barracuda Spam Firewalls, the basic MX record protocol will deliver email to the units that have not failed automatically. Once the failed Barracuda Spam Firewall is brought back online, it will begin accepting mail automatically. If you use a Load Balancing Device, the system will behave similarly. The load balancer will know if one of the Barracuda Spam Firewalls is not responding and will route all of the inbound mail traffic to another machine. This type of failover is also automatic and immediate.