

High availability and fault tolerance are essential in modern enterprise and service provider networks. Clustering Barracuda Spam & Virus Firewalls enables organizations to meet their high availability and fault tolerance requirements while also providing centralized management of policy, scalability and data redundancy.

Linking multiple Barracuda Spam & Virus Firewalls is easy to do with a few parameter settings, and once you configure one of the devices, configuration settings are synchronized across the cluster almost immediately. Clustered systems can be geographically dispersed and do not need to be located on the same network.

Benefits of Clustering the Barracuda Spam & Virus Firewall

Centralized Policy Management

You can configure your spam, virus, and custom email delivery policies from any Barracuda Spam & Virus Firewall in the cluster – all changes are immediately replicated to the other Barracuda Spam & Virus Firewalls in the cluster.

Alternatively, you can designate one Barracuda Spam & Virus Firewall as the “host” from which users will access their quarantined email on the cluster. To do this, you would simply set that device to be the “Quarantine Host” and not direct any email traffic to it. There are two benefits to this configuration:

- Enables you to tighten security by restricting Web interface access to only one Barracuda Spam & Virus Firewall in the cluster
- Optimizes performance of the Web interface by isolating it from the impact of spikes in email volume on the network

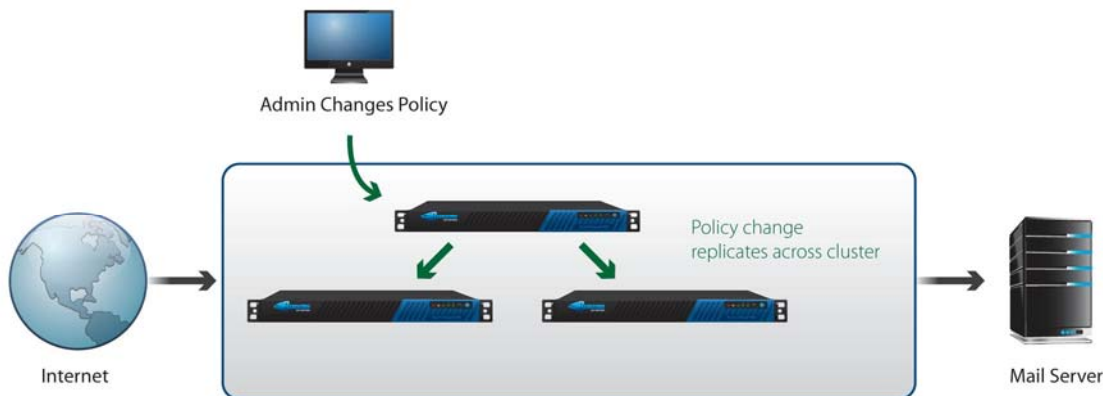


Figure 1 – Centralized policy management

Data Redundancy and Guaranteed Configuration Updates

Quarantined messages are replicated across the cluster such that each user has a primary quarantine inbox on one Barracuda Spam & Virus Firewall and a secondary inbox on another Barracuda Spam & Virus Firewall. This redundancy and fault tolerance ensure that all user data remains available if a single node in the cluster fails.

Barracuda Spam & Virus Firewall clusters are also fault tolerant to temporary network failures or delays because all cluster events and updates are queued on each node. Each individual Barracuda Spam &

Virus Firewalls continues to process email independently and automatically synchronizes quickly as network communications allow.

Federated Search

Clustering Barracuda Spam & Virus Firewalls provides you with a centralized view of all messages in a cluster through a distributed database architecture. With federated search, you can locate any messages across the cluster by issuing a query from any single Barracuda Spam & Virus Firewall. Unlike centralized database architectures that involve network traffic for all processed messages, this distributed database architecture restricts network traffic to only messages returned with query results.

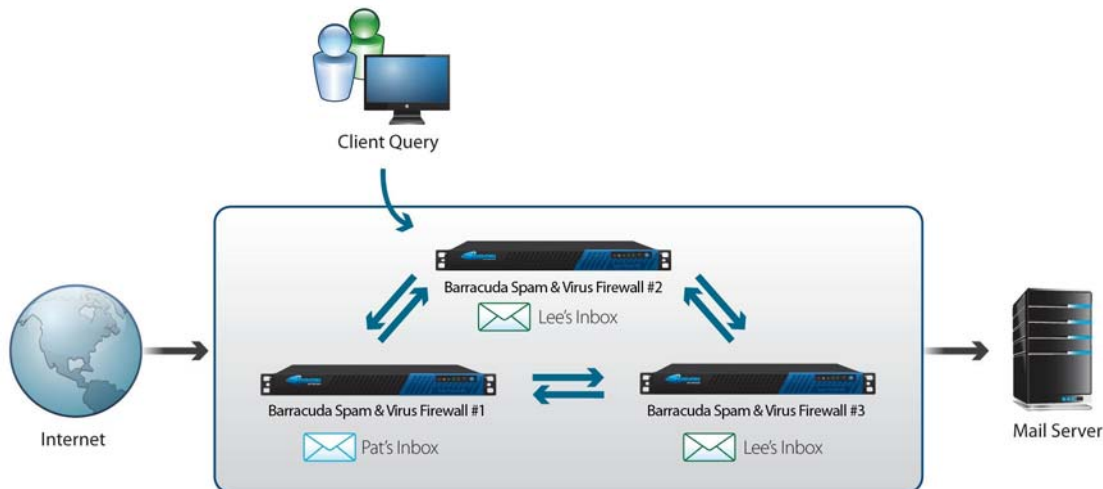


Figure 2 – Federated search across the cluster

Scalability

Because Barracuda Spam & Virus Firewall clustering leverages a distributed database architecture, it is very simple to implement and is easily scalable. As your email traffic volume grows, you can simply add one or more additional Barracuda Spam & Virus Firewalls. Note that clustering is supported on Barracuda Spam & Virus Firewall models 400 and higher, and each Barracuda Spam & Virus Firewall in the cluster must be the same model number.

Secure Access and Data Transmission

Barracuda Spam & Virus Firewall clustering utilizes encrypted and secure communications for user access, message replication and configuration synchronization across the cluster.

Limiting User Access

As mentioned above, you can choose to dedicate a single Barracuda Spam & Virus Firewall in the cluster as the Quarantine Host to serve up the end-user interface through which users will access their quarantine inboxes, even though their actual quarantine inbox (primary or secondary) may be hosted by another Barracuda Spam & Virus Firewall in the cluster. Network security is enhanced by limiting end-user access (port 8000 by default) and administration to only one Barracuda Spam & Virus Firewall on the Internet. In this configuration, quarantine notifications from all appliances in the cluster will direct users to that Quarantine Host, and you would direct all email to the **other** nodes on the cluster.

Secure Message Transmission

Data transmission is always encrypted through SSL communication between Barracuda Spam & Virus Firewalls in the cluster. Secure communication is controlled over defined TCP ports.

Restricted Access to Configuration

Transmission of configuration data between devices on the cluster is secured by a shared password, or “shared secret”, which the administrator creates and assigns to every Barracuda Spam & Virus Firewall. This prevents access to configuration parameters from other Barracuda Spam & Virus Firewalls outside the cluster or other network devices.

Easy Deployment

Deploying clustered Barracuda Spam & Virus Firewalls is easy with the step-by-step instructions documented in the user interface. Every Barracuda Spam & Virus Firewall in a cluster must be the same model and have the same version of firmware installed.

To cluster Barracuda Spam & Virus Firewalls:

- Completely configure one Barracuda Spam & Virus Firewall (we’ll call this the “Original Node”) with spam, virus, and custom email delivery policies. Set a cluster “shared secret.”
- To join another Barracuda Spam & Virus Firewall to form a cluster, configure the network, time zone, and password on that node (we’ll call this the “First Join”), then enter the IP address and the shared secret of the “Original Node.” As soon as the “First Join” node is added, the policies and configuration parameters of the “Original Node” will be replicated to that node.
- Adding subsequent nodes follows the same procedure.

Directing Email to the Cluster: Load Balancing

You can load balance incoming email directed to a cluster of Barracuda Spam & Virus Firewalls in one of two ways:

- 1) Use a [Barracuda Load Balancer](#) to direct email into the cluster. The Barracuda Load Balancer can distribute traffic based on weighted round-robin, weight least connections, or adaptive scheduling methods that query each Barracuda Spam & Virus Firewall for load and distribute traffic accordingly.
- 2) Configure multiple DNS MX records. Generally, MX record load balancing will not distribute the traffic as evenly as a dedicated load balancer. See the Barracuda Networks white paper entitled [Load Balancing Using DNS MX Records](#) for more information.