

Benefits of Clustering the Barracuda Email Security Gateway

<https://campus.barracuda.com/doc/3866655/>

Clustering Barracuda Email Security Gateways 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 Email Security Gateways 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.

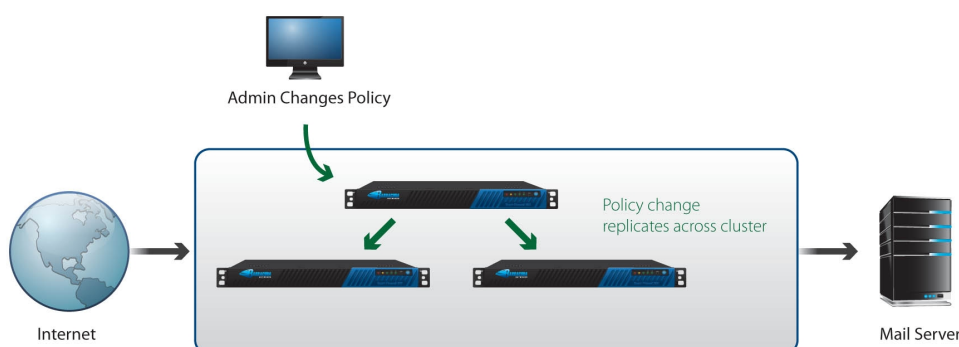
Centralized Policy Management

You can configure your spam, virus, and custom email delivery policies from any Barracuda Email Security Gateway in the cluster – all changes are immediately replicated to the other Barracuda Email Security Gateways in the cluster.

Alternatively, you can designate one Barracuda Email Security Gateway as the “host” from which to perform administration of 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 Email Security Gateway 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

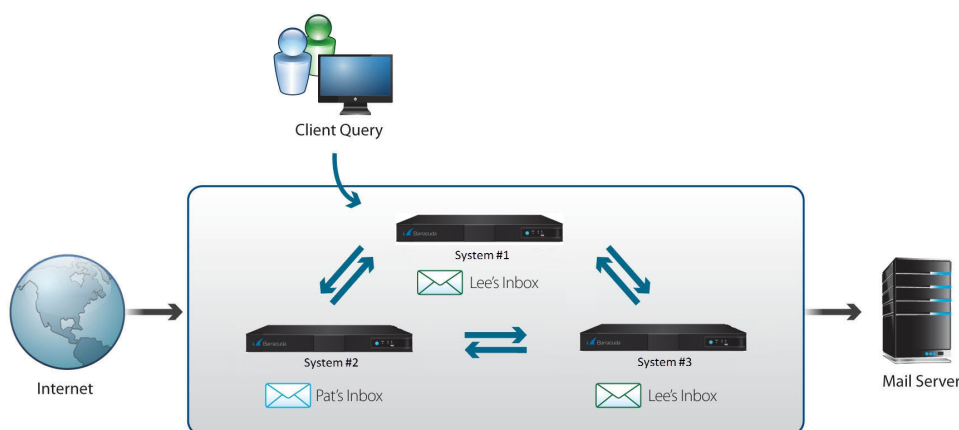
Quarantined messages are replicated across the cluster such that each user has a primary quarantine inbox on one Barracuda Email Security Gateway and a secondary inbox on another Barracuda Email Security Gateway. This redundancy and fault tolerance ensure that all user data remains available if a single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

Barracuda Email Security Gateway 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 Email Security Gateway continues to process email independently and automatically synchronizes quickly as network communications allow.

Federated Search

Clustering Barracuda Email Security Gateways 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 Email Security Gateway. 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 Email Security Gateway 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 Email Security Gateways. Note that clustering is supported on Barracuda Email Security Gateway models 400 and higher, and each Barracuda Email Security Gateway in the cluster must be the same model.

Secure Access and Data Transmission

Barracuda Email Security Gateway 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 one Barracuda Email Security Gateway on the cluster as the “Quarantine Host” to limit users’ access to that node when checking their quarantine inboxes. In this configuration, quarantine notifications from all Barracuda Email Security Gateways in the cluster will direct users to that Quarantine Host, and you would direct all email to the **other** nodes on the cluster.

Data transmission is always encrypted through SSL communication between Barracuda Email Security Gateways 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 Email Security Gateway. This prevents access to configuration parameters from other Barracuda Email Security Gateways outside the cluster or other network devices.

To cluster Barracuda Email Security Gateways

Deploying clustered Barracuda Email Security Gateways is easy with the step-by-step instructions documented in the user interface. Every Barracuda Email Security Gateway in a cluster must be the same model and have the same version of firmware installed. For complete detailed instructions in the Barracuda TechLibrary, see [How to Cluster the Barracuda Email Security Gateway](#).

Directing Email to the Cluster: Load Balancing

You can load balance incoming email directed to a cluster of Barracuda Email Security Gateways in one of two ways:

1. Use a [Barracuda Load Balancer ADC](#) to direct email into the cluster. The Barracuda Load Balancer ADC can distribute traffic based on weighted round-robin, weight least connections, or adaptive scheduling methods that query each Barracuda Email Security Gateway 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.

Figures

1. centralized_policy_m.JPG
2. Federated_search.JPG

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.