Solution Brief

Deploying Barracuda Web Security Gateway Clusters with the Barracuda Load Balancer ADC

Challenges

- Deploying multi-model Barracuda Web Security Gateway clusters due to growth in Internet traffic
- Maintaining Barracuda Web Security Gateway cluster performance
- Efficient usage of existing Barracuda Web Security Gateway devices

Solution

- Barracuda Load Balancer ADC
- Included Global Server Load Balancing (GSLB), Session Persistence, Application Security, and SSO
- Up to 15Gbps throughput
- Physical and virtual form factors

Benefits

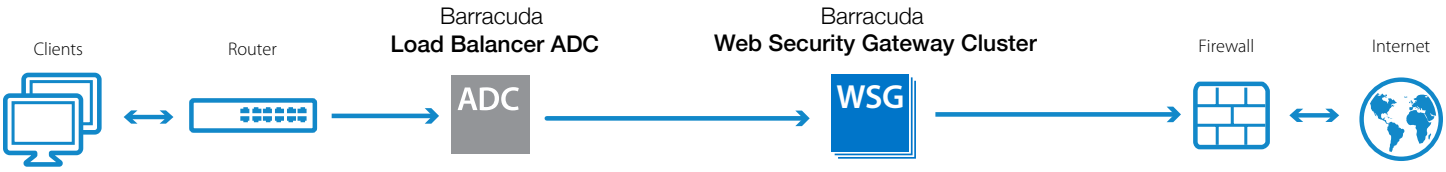
- Performance-aware load balancing improves the performance of the Barracuda Web Security Gateway cluster
- Performance-aware load balancing ensures quicker Internet access via the Barracuda Web Security Gateway cluster
- Provides redundancy for the Barracuda Web Security Gateway cluster

Introduction

The Barracuda Web Security Gateway lets organizations benefit from online applications and tools without exposure to web-borne malware and viruses, lost user productivity, and misused bandwidth. As a comprehensive solution for web security and management, it unites award-winning spyware, malware, and virus protection with a powerful policy and reporting engine.

Due to an increasing number of users needing to access the web, organizations seek to augment their Barracuda Web Security Gateway deployments by clustering additional devices to their existing deployment. In such growing deployments, there may be a mix of Barracuda Web Security Gateway hardware models — from the lower end devices that the organization started with, to newer, more capable Web Security Gateway devices that can handle higher traffic loads. The issue with such clustering is in the distribution of the web traffic load across the various Web Security Gateways. A router would typically distribute all the web traffic evenly across all the devices, without considering the capability of the devices. This can lead to performance issues.

The Barracuda Application Delivery Controller



The Barracuda Load Balancer ADC enables organizations to add scalability, redundancy, and security to applications in their data centers with a single, integrated and cost-effective platform. When used with the Barracuda Web Security Gateway, it provides performance-aware load balancing and redundancy. This ensures higher performance from the Barracuda Web Security Gateway cluster — all without breaking the IT budget.

The Load Balancer ADC is deployed in between the clients of the Web Security Gateway cluster and distributes traffic across the various devices in the cluster. Using its built-in load-balancing algorithms, the ADC will perform performance-aware traffic distribution across the devices in this cluster. The Barracuda Load Balancer ADC queries each of the connected Barracuda Web Security Gateway devices in the cluster for performance and load information. The load-balancing algorithm will then send traffic to the devices with lesser load, improving the efficiency of the Barracuda Web Security Gateway.

By ensuring that the Web Security Gateway cluster is performing at its best, the Barracuda Load Balancer ADC enables faster Internet access through the cluster. In case one of the nodes in the Barracuda Web Security Gateway Cluster fails, the Barracuda Load Balancer ADC will remove this device from the load balancing scheme and direct traffic across other devices.

Configuration of the Barracuda Web Security Gateway devices in a cluster is simple. Administrators can easily configure all devices in the cluster by using the link management configuration and synchronize the configuration across all the devices in the cluster.

Application Delivery with Barracuda

Designed for today's high-traffic data centers, the Barracuda Load Balancer ADC is a high-performance application delivery controller that combines application acceleration, availability, and control with advanced security capabilities. Deployed by thousands of organizations worldwide, the Barracuda Load Balancer ADC is a robust, proven solution that manages and secures billions of application transactions daily. It's available as a multiport platform with fiber and copper network interfaces, as well as a virtual appliance.

To learn more about upgrading your Forefront TMG installation to Barracuda's Application Delivery Controller solution, visit www.barracuda.com/ADC. Or call 1-408-342-5400 or 1-888-268-4772 (US & Canada) to request a free 30-day trial.

About Barracuda Networks, Inc.

Protecting users, applications, and data for more than 150,000 organizations worldwide, Barracuda Networks has developed a global reputation as the go-to leader for powerful, easy-to-use, affordable IT solutions. The company's proven customer-centric business model focuses on delivering high-value, subscription-based IT solutions for security and data protection. For additional information, please visit www.barracuda.com.