IMPERVA®

Imperva Incapsula Load Balancer

DATASHEET

Optimize Traffic Distribution and Application Delivery from the Cloud

The Incapsula Load Balancer enables organizations to replace their costly appliances with an enterprise-grade cloud-based application delivery solution. Based on a global CDN, the Load Balancer supports a single data center with multiple servers, site failover (for DR scenarios), and Global Server Load Balancing (GSLB). Real-time health monitoring and notifications ensure that traffic is always routed to a viable web server.

What You Get

- Application level Load Balancing solution for optimal resource utilization
- Built-in flexibility to support single data center, multiple data centers (GSLB) and disaster recovery scenarios
- Application Delivery Rules to intelligently route traffic
- Real-time monitoring and failover capabilities for high availability

Intelligent Application Level Load Balancing

Through real-time monitoring of actual HTTP requests to each server, application level load balancing intelligently distributes the load among servers. By understanding the actual flow of traffic to each server, Incapsula guarantees optimal resource utilization. Other load balancing methods, such as Layer 3 and DNS-based load balancing, are not able to provide true load balancing because they do not monitor the actual traffic. Unlike DNS-based load balancing, which is TTL-dependent, routing changes in Incapsula are immediate and across-the-board for all users. A variety of traffic distribution methods is supported, all of which are session-persistent.

Why Incapsula?

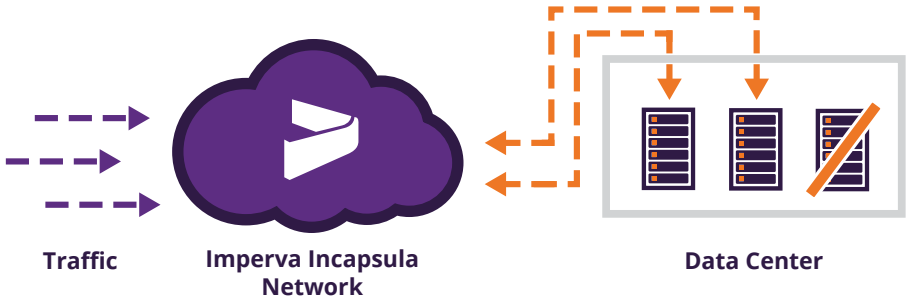
- Cloud-based load balancing for fast and cost-effective scalability
- Optimal traffic distribution for enhanced application performance and reduced server loads
- Client Classification identifies bots and enables targeted rerouting
- Activated by simple DNS change - no hardware or software installation, integration or changes to the website

Meeting All Your Load Balancing Needs

The Incapsula Load Balancer supports the following:

Server Load Balancing

Incapsula balances traffic across multiple web servers within a data center directly from the cloud. This allows websites and applications to cost-effectively scale their operations without requiring a local load balancing appliance or virtual appliance. Acting as a dedicated load balancer for the target website or application, Incapsula accurately balances traffic between servers according to load, while removing non-responsive servers from the pool.



Incapsula supports various load balancing methods. By default, all of these methods are also session-persistent, meaning the same HTTP session will always return to the same preferred server (if it is responsive). The website administrator can select one of the following distribution options when setting up the service:

- **Least Pending Requests**

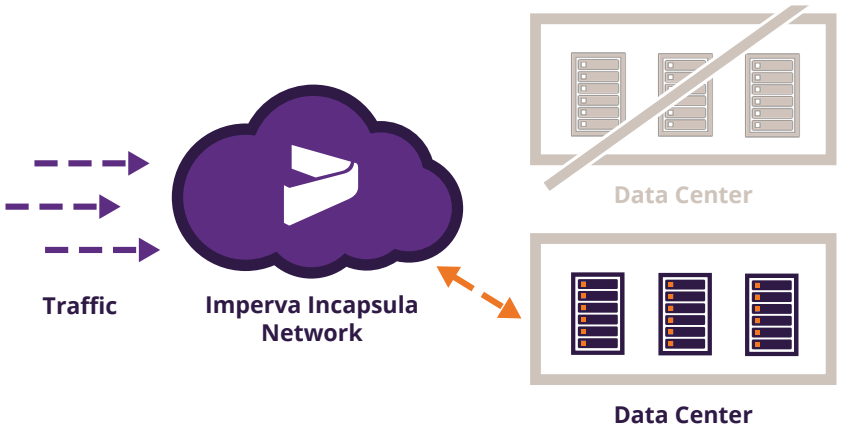
  The most accurate way of ascertaining the load on the server is by measuring how many HTTP requests it is currently processing. This enables distribution of the load according to the real time load on the server.

- **Least Open Connections**

  This method distributes traffic by forwarding requests to the web server that has the smallest number of open connections.

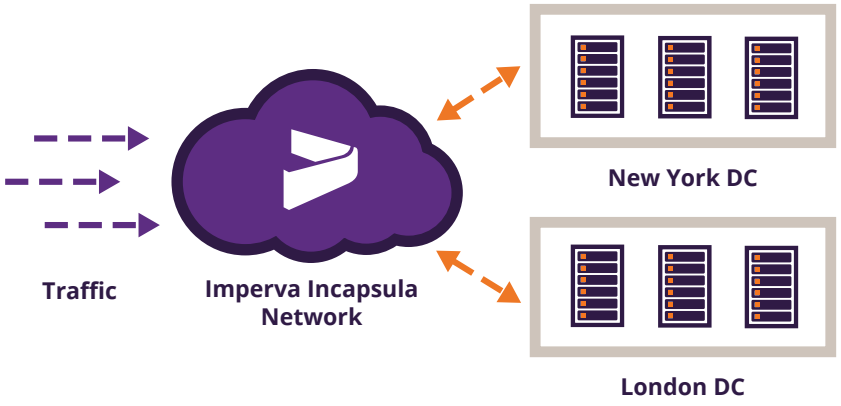
Site Failover (Disaster Recovery)

Incapsula supports automatic failover between primary and secondary sites to accelerate disaster recovery in the event of an outage. As soon as Incapsula detects that the primary site has gone down, it automatically kick-starts the standby data center. Incapsula's real-time health monitoring enables immediate detection of outages to ensure high availability even in the case of a catastrophic failure.



Global Server Load Balancing (GSLB)

Global server load balancing for organizations operating multiple data centers ensures high availability and consistent performance of applications and websites.



Leveraging a global CDN, Incapsula performs global load balancing using the following methods:

- **Best Connection Time**
  Incapsula samples the network connection times between Incapsula and the customer's data centers on a periodic and frequent basis. Based on this sampling, traffic is sent to the data center with the best connection time.
- **Geo-Targeting Preferred**
  This method enables website owners to set their own policy for routing traffic to a particular data center based on the visitor's geographical location. For example, an organization may wish to serve different content (for example, ads) to different end users based on their location. Under this method, if the preferred data center is unavailable for any reason, Incapsula re-routes the traffic to an available one.
- **Geo-Targeting Required**
  This geography-based load balancing method is similar to Geo-Targeting Preferred. However, using this method, if the required data center is unavailable, the traffic is null routed. This method is used by international organizations that maintain multiple data centers in different countries to comply with regulatory issues.

Application Delivery Rules

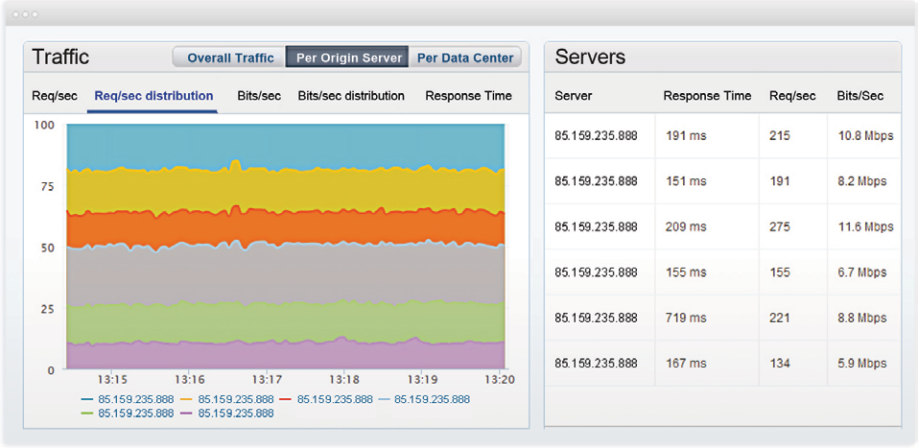
Rewrite, forward or redirect requests at the edge and return different assets based on Incapsula intelligence and request attributes, without changing the client-facing URL.

- Switch content and redirect users based on layer 7 attributes, such as URL patterns, cookies, HTTP headers, and client classification attributes.
- Improve user experience and SEO ranking by rewriting relative and dynamic URLs to clean customer-facing URLs.
- Offload connections and reduce round trip times between your web server and other backend servers.
- Leverage Incapsula client classification to identify bad bots and redirect them to a special site or server with fake content.
- Define rules based on client behavior, using customizable rate thresholds for various parameters.
- Implement backend logic without changing application code.
- Extend role-based control to non-technical users.

Monitoring and Alerts

Health Monitoring

Real-time health and performance checks of server activity are used to detect outages and eliminate downtime. In this way, Incapsula ensures that traffic is always routed to a viable web server. Passive monitoring is used to evaluate server responses to the actual traffic that is forwarded to them. The determination that a server is down is based on an extensive set of user-configurable parameters, which can be fine-tuned to the specific needs/policies of each organization. These include, for example, what is considered an error, the amount of errors in a given time period that constitute a "failure", etc. Once a server has been flagged as "down", Incapsula performs active verification checks to determine whether the server has resumed operation. Active verification is based on sending a dedicated HTTP request to a predefined URL and checking whether the expected response is received. If so, the load balancer will renew the flow of traffic to it.



IMPERVA INCAPSULA

Alerts

Incapsula Users can receive email alerts to notify them of virtually any possible failover scenario.

The Incapsula management console allows users to fine-tune the sensitivity of the precise scenarios that will trigger an alert. For example:

- Specific server is down
- Data center is down
- Flexible parameters such as number of proxies re-routing traffic, etc.