Guide

Akamai to Incapsula Migration Guide

IMPERVA Incapsula

Introduction

Incapsula is an enterprise-grade cloud service that helps companies deliver applications more efficiently and securely. This is accomplished through four seamlessly integrated core sub-services: a Content Delivery Network (CDN), website security, DDoS protection and load balancing. Leveraging a multi-layer approach and product set, the Incapsula service accelerates the delivery of web content and protects applications from external threats and attacks.

The purpose of this guide is to help enterprises achieve a successfully migrate from Akamai's CDN to the Incapsula CDN. It is intended for Akamai customers who have decided to leave Akamai's CDN and are planning their transition to the Incapsula CDN.

This document provides practical guidance for planning and executing migrations of websites and applications from the Akamai network onto the Incapsula network. In addition to providing basic information about configuring and setting up the Incapsula service, this guide also outlines the key similarities and differences in the way the services work, so you can better understand what to expect when you move to Incapsula.

Basic Configuration

Scoping

For both Akamai and Incapsula, the definition of a site is the same. Each site is defined by a DNS record, known as a CNAME, which represents a domain or subdomain (e.g., www.example.com, blog.example.com). The CNAME is provided by Incapsula when you migrate to the service. You will also receive an IP record for your top level (naked) domain (e.g., example.com).

Supporting SSL Traffic

If you are using the Kona Web Application Firewall to inspect and filter SSL traffic, you may recall that adding the SSL support required a rather lengthy process that typically takes up to one month.

For enterprises migrating to Incapsula, setting up support for SSL certificates is simple, fast (usually within 24 hours) and free of charge. You can upload your own SSL certificate using the Incapsula customer self-service portal, or generate a new certificate via Incapsula.

During system activation, Incapsula automatically identifies websites that support SSL traffic (HTTPS) and leads you through a simple setup process for those sites. This process generates a certificate for your domain that will be hosted on our servers. During the setup process you are requested to approve the creation of such a certificate by our certificate provider.

The process of adding SSL support involves three simple steps:

1. Within 24 hours of adding the website you will receive an email from one of our SSL Certificate Authority partners, requesting approval to generate an SSL certificate for your domain. To approve this request simply reply with "yes" in the message body.

2. After your approval Incapsula will provision the service to support SSL on your domain. This process can take up to 24 hours.

3. Once the process is completed, you will be notified by email and you will be able to proceed to the final step of adding your website to the Incapsula service.

Client IP Tracking

Many application owners need to track the IP addresses of their visitors. This becomes more complicated when the application is delivered via proxy servers on a CDN, since the application sees the proxy's IP address rather than the client's real IP.

The X-Forwarded-For (XFF) HTTP header field is the de facto standard (RFC) for identifying the originating IP address of a client connecting to a web server through an HTTP proxy or load balancer. The main drawback of XFF is that if your traffic passed through three proxies, three headers are added to your webpage, which adds complexity for your application.

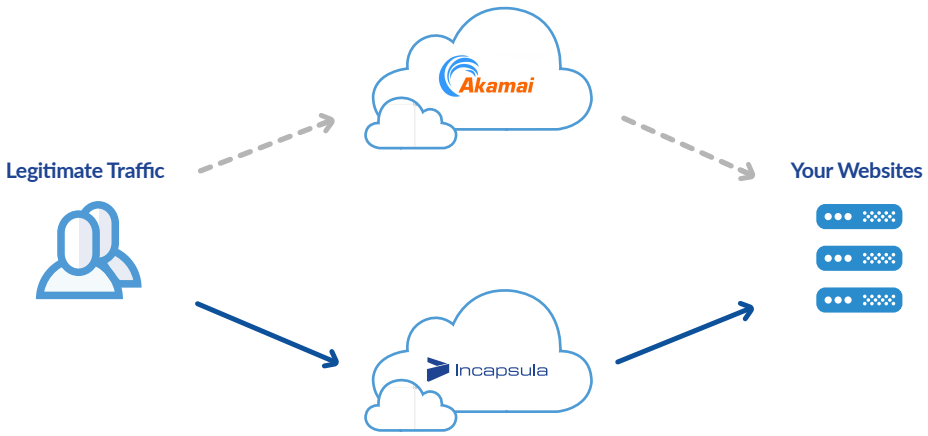
For this reason CDNs like Akamai and Incapsula use proprietary headers rather than the standard XFF format. Akamai customers typically do this with a header called "True Client IP," which can be customized as needed.

The Incapsula version of this proprietary header is known as "Incap-Client-IP", and is provided free of charge. In order to keep using the header name you used on Akamai (and to avoid making changes to your applications), you can customize the "Incap-Client-IP" header name to "True Client IP" using the Incapsula configuration settings.

Transition Process

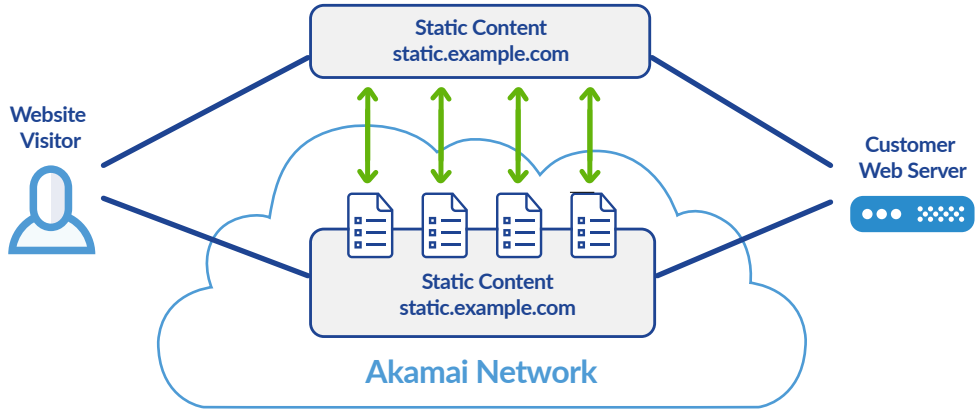
Incapsula and Akamai use DNS redirection to persistently re-route incoming traffic (HTTP/HTTPS) through the CDN. Thus, migrating website and application traffic to Incapsula is a simple matter of setting the sites up in Incapsula, then making the necessary DNS change.

It should be kept in mind that customers using Akamai's Managed DNS service in conjunction with its CDN will most likely prefer to find a new DNS provider. Incapsula, for its part, can work with any DNS provider (many are free). Once you've chosen your new DNS provider, the relevant entries need to be set to point your traffic to Incapsula.



Transitioning Static and Dynamic Domains

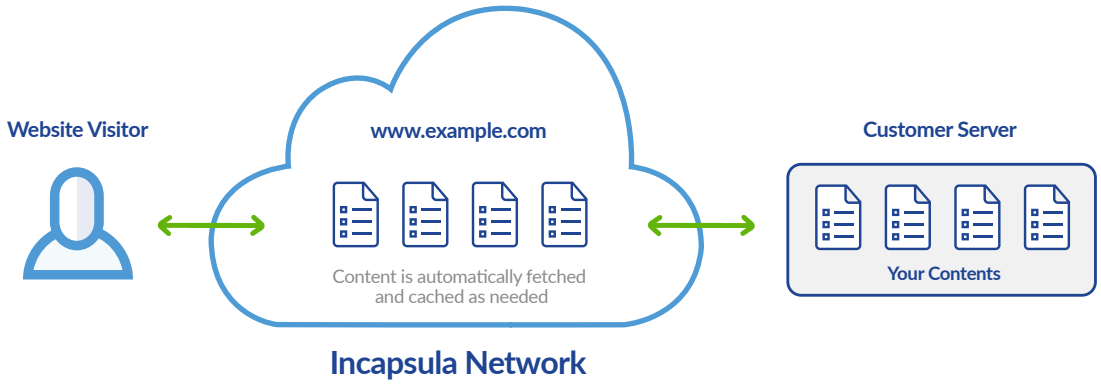
To support Akamai's caching capabilities, many Akamai customers have split their applications in such a way that static content is sent to one subdomain and dynamic traffic is sent to another. The static content is then sent through Akamai's CDN, while the dynamic content is neither accelerated nor secured by Akamai. This type of configuration allows the dynamic site to call the static content directly from Akamai's network (see diagram below).



In contrast to Akamai, the Incapsula CDN is built to analyze and cache both static and dynamic traffic, so there is no need to break out traffic by type (static/dynamic). Content is fetched as needed and stored on Incapsula. The content is refreshed periodically based on user defined cache settings.

Incapsula further simplifies website optimization through the use of a proprietary algorithm which dynamically learns what resources are cacheable, and for how long. This algorithm continuously profiles website resources, identifying dynamically-generated resources which are in essence static as they do not change over time and for different users. These resources are then cached to significantly reduce page load times and reduce server loads, as these files require the lion's share of the computing power.

When migrating your content to Incapsula, you have the choice of keeping your existing Akamai setup and simply putting both domains on the Incapsula cloud. Alternatively, you can merge them into a single domain for easier maintenance over the long run. Incapsula supports both scenarios.



Security

The Kona Web Application Firewall is an integral part of Akamai's CDN offering, providing application layer defense against SQL injection, cross-site scripting and other types of web attacks that can result in data theft. When migrating your websites or applications from Akamai's CDN, it is important to make sure that the new CDN also provides the highest level of web application security.

Web Application Firewall

The Incapsula service includes a PCI-compliant, enterprise-grade web application firewall with similar functionality to what you had with Kona. For a high-level feature comparison, see the table below:

Feature	Akamai	Incapsula
Certified Gartner Magic Quadrant leading PCI-compliant WAF		✓
Access control (white/blacklisting)	✓	✓
IP reputation-based monitoring system	✓	✓
API integration	✓	✓
Client classification algorithms to mitigate advanced bots		✓
Transparent progressive challenges for minimal user impact and reduced false positives	✓	✓
Backdoor protection to guard against malware infection		✓
Two-factor authentication to prevent breach by stolen passwords		✓
Self-service customization of security rules		✓
60-second security rule propagation		✓
Productized SIEM integration with pre-made dashboards		✓

A more detailed feature-to-feature comparison of the CDNs can be found here: https://www.incapsula.com/incapsula-vs-akamai.html

Some of the key differences between the Kona and Incapsula WAFs are described in more details in the following pages.

Custom Security Rules

Many Akamai users have implemented custom security rules to allow for faster response and more flexible enforcement of their organizations' security policies and use cases.

As custom rule creation is typically performed by Akamai's Professional Services team, the turnaround time for rule creation and propagation across Akamai's network can take days or weeks.

Our answer to this is IncapRules. IncapRules, is a proprietary scripting language that allows users to implement their own security and access control rules – on demand – on top of the existing Incapsula security logic. These rules are created via a dedicated GUI that is specially designed to simplify the rule generation process. Mirroring the Incapsula security-oriented approach, custom rules can be propagated system-wide within 60 seconds.

When migrating from Akamai, there is no programmatic way to transition existing custom security rules to Incapsula. We recommend to download an XML file from Kona with all the custom rules. Then, re-create these rules in Incapsula using the intuitive and user-friendly IncapRules editor. Alternatively, the Incapsula Professional Services team can be hired to perform the initial bulk custom rule creation.

IP Reputation and Client Classification

Kona's Client Reputation feature crowdsources feeds of IP addresses and assigns scores based on their propensity to perform malicious activities such as web application attacks, DDoS attacks and vulnerability scanning. The scores reflect prior behavior as observed over the Akamai network and analyzed by Akamai's security intelligence platform. Based on the reputation score of the IP address, Kona automatically allows, alerts or blocks the incoming traffic.

If you've been using Kona's Client Reputation feature to improve your security decisions, you can achieve similar results using the Incapsula enhanced IP Reputation and Client Classification features (which are available free of charge as part of the WAF).

Incapsula combines crowdsourced data from its own network (comprising hundreds of thousands of websites) with a big data analytics platform that monitors attack vectors and signatures, attacker IPs, malicious bots (e.g., PushDo or Cyclone) and botnet signatures.

These capabilities are complemented by the Incapsula client classification engine that analyzes traffic in real time. This is critical when it comes to distinguishing legitimate website visitors (humans, search engines, etc.) from automated or malicious bots. The client classification engine identifies bots based on header data, IP addresses and ASN numbers, behavior monitoring, client technology fingerprinting and more.

Once a bad bot is identified, a signature is created for it. This means the next time this bot comes to visit any site protected by Incapsula, it will be immediately blocked. Moreover, the reputation of the attacking IP is also recorded and added to the IP reputation database.

Integration and API Access

Akamai customers are typically provided API access to facilitate integration with their own backend systems. Similarly, the Incapsula service comes with an API that enables enterprises to streamline customer provisioning and account management.

In addition, to enrich your existing security event management workflows, Incapsula has developed a "productized connector" for seamless integration with several leading SIEM platforms, including HP ArcSight, Splunk, and McAfee. This product is designed to provide turnkey SIEM integration without the need for professional services, consultants, or specialized IT expertise.

This connector resides on the customer's network, and serves as a link between the SIEM and the Incapsula API. In addition to near real-time event reporting and strong data encryption, this offering includes pre-made custom dashboards and reports for easy viewing of incoming data from within the SIEM according to security best practices.

Performance

In terms of their approach to content caching, there are differences in functionality between Akamai and Incapsula. While both CDNs support most major use cases, their approaches to content caching differ as described in the sections below.

Akamai Content Caching Use Cases

1. "Push CDN" for Very Large Static Files

The "Push CDN" model is typically used by developers to distribute applications and new software versions to users. These very large files are "pushed" (i.e., uploaded) by developers to the CDN, where they are available for download by users from the closest available POP.

Akamai's CDN is used by numerous companies to support this use case. Incapsula, on the other hand, was built to work with websites and applications and hence does not support the "Push CDN" model.

2. Static Content Relevant to Website or Application

Akamai's caching options are optimized for delivery of large static files, such as graphic images. Akamai supports static content caching by creating a new domain (e.g., static.example.com) containing all static content. Client websites link to the static domain and retrieve the cached content as needed. For websites containing both static and dynamically-generated content, this use case requires maintaining separate domains for the static and dynamic content.

Incapsula can support this use case, and enables Akamai users to migrate both domains "as is" to the Incapsula cloud.

3. Dynamic Content Caching

Dynamically-generated content—the type often found on modern script-generated websites, SaaS (software as a service) and other highly-personalized web applications – requires more sophisticated capabilities than static content. Due to the sensitive data used by today's dynamic applications, this type of content requires both acceleration and security.

Akamai's Dynamic Site Accelerator (DSA) feature is used by some clients to support dynamic content caching. DSA pulls and caches fresh content continuously onto servers that are close to the end user, relying heavily on network optimization and compression techniques to reduce latency.

Incapsula was built from the ground up to support dynamic content delivery, and uses intelligent caching methods to provide a comprehensive acceleration solution. For instance, it utilizes advanced traffic profiling algorithms to auto-identify and cache dynamically-generated content and to serve that content directly from memory.

4. Video Streaming

Akamai specializes in video streaming and offers unique capabilities, such as live video streaming, not supported by Incapsula. Akamai supports complete video file caching, as well as caching file ranges to enable users to "jump" within a video file.

Incapsula is able to cache complete video files, but does not support caching of file ranges like Akamai does. Customers migrating from Akamai with video streaming needs should use a dedicated streaming service alongside Incapsula.

Incapsula provides an equivalent solution for most major use cases:

Akamai Use Case	Incapsula Equivalent
Push CDN	Not Available
Static Content Caching	Incapsula CDN
Dynamic Content Caching	Incapsula CDN
Video Streaming	Not Available

A feature-to-feature comparison of the CDNs can be found here:
https://www.incapsula.com/incapsula-vs-akamai.html

Load Balancing

Akamai provides local server load balancing capabilities using cloud-based application-layer load distribution. These capabilities include control and real-time monitoring options, several choices of load balancing algorithms, and local server failover. Akamai also offers a DNS-based global traffic management solution for GSLB and site failover.

The Incapsula application-layer local server load balancing is very similar to that of Akamai, enabling an easy transition for Akamai customers. It supports a variety of session-persistent load balancing methods that intelligently distribute the load among servers based on the actual flow of traffic.

If you maintain multiple data centers, Incapsula also offers a highly effective GSLB solution to meet your needs. Routing decisions are based on real-time analysis of HTTP requests, allowing for a range of distribution algorithms, including "best connection time" and geo-targeting. Rather than relying on DNS, Incapsula leverages its reverse proxy network to enable immediate re-routing as conditions change.

With respect to disaster recovery, the Incapsula Site Failover solution uses application-layer load balancing to eliminate the TTL-related delays and uneven performance characteristic of DNS-based solutions.

Migration Planning Checklist

The following checklist can be used as a guide to make sure you cover all the bases in planning and executing your transition from Akamai to Incapsula.

1. Scoping

- [ ] Perform basic scoping by answering the following questions about your environment.
- [ ] How many sites do you wish to secure and accelerate?
- [ ] How much aggregate bandwidth will they have?
- [ ] Do you need additional DDoS Protection?
- [ ] Do you want to enable two-factor authentication to protect your websites' admin areas?

  If yes, how many users will need access? _____

- [ ] Will you be using load balancing?

  If yes, how many Data centers?_____

2. Transition

- [ ] Create Incapsula account
- [ ] Configure sites to be transitioned in the Incapsula UI
- [ ] Set up SSL certificates for sites
- [ ] Make DNS changes to redirect site traffic through Incapsula

3. Advanced Setup

- [ ] Configure caching and optimization rules to maximize website performance
- [ ] Create custom security rules using the IncapRules engine
- [ ] Set up load balancing (to support complex deployments)

If you need further assistance with your transition to Akamai, please visit us at http://support.incapsula.com or contact our Support team 24/7 at support@incapsula.com.

T: +1 (866) 250-7659 | E: info@incapsula.com | www.incapsula.com
3400 Bridge Parkway, Suite 200, Redwood Shores, CA 94065

IMPERVA®
Incapsula