Secure Content Delivery Network

Updated: 2014 February 18

Akamai provides market-leading managed services for powering rich media, dynamic transactions, and enterprise applications online. Having pioneered the content delivery market one decade ago, Akamai's services have been adopted by the world's most recognized brands across diverse industries. The alternative to centralized Web infrastructure, Akamai's global network of tens of thousands of distributed servers provides the scale, reliability, insight and performance for businesses to succeed online. An S&P 500 and NASDAQ 100 company, Akamai has transformed the Internet into a more viable place to inform, entertain, interact, and collaborate. To experience The Akamai Difference, visit www.akamai.com.

US Headquarters 8 Cambridge Center Cambridge, MA 02142

www.akamai.com

Tel: 617.444.3000 Fax: 617.444.3001 US Toll free 877.4AKAMAI (877.425.2624)

Akamai Technologies, Inc.

For a list of offices throughout the world, see:

http://www.akamai.com/html/about/locations.html

Network Overview

Network

SSL content is delivered over a dedicated portion of the Akamai network, segregated physically and logically from the rest of the Akamai's systems. This dedicated network, the Akamai Secure Content Delivery Network, is composed of groups of servers deployed and physical requirements designed to comply with the Payment Card Industry Data Security Standards (PCI DSS). The Akamai edge servers deliver SSL content to end-users on behalf of Akamai's customers.

Regions

A group of edge servers is referred to as a *region*. Akamai has hundreds of regions distributed around the world.

Region hardware includes the following:

Hardware	Description
Locked cabinets	Cabinets are locked with electronic safe locks. The combinations for these cabinets are managed by Akamai personnel. Each cabinet door is equipped with a camera.
Cameras	The cameras are programmed to detect changes in light or motion and to record access to the cabinet. The Akamai NOCC receives automatic alerts including the images captured by the cameras should they be triggered by a change in their environs.
Servers	Rack-mounted computers are specific models purchased by Akamai from a small number of qualified suppliers. Participation in the Secure Content Delivery Network is only available after the Akamai NOCC accepts the region, the latest software release is installed, and the machines are audited to receive appropriate encryption keys.
Network Switches	Network switches provide Ethernet (Layer-2) and IP connectivity to the servers.

Edge Servers

It is important to note that Akamai personnel do not require access to our customer's internal systems. Akamai edge servers operate as surrogate web servers pulling content from the origin site using standard protocols such as HTTP and HTTPS, and do not have any access to the back-end systems of the customer's hosted facility. The edge server proxies the end-user's HTTP/HTTPS request to the customer's website, and will make the same end-user request to the origin web servers at the customer's hosted facility for the purpose of retrieving content.

How It Works

Establishing and Maintaining Secure Sessions

The procedures for establishing and maintaining secure sessions are as follows:

1. The customer completes a certificate request to authorize Akamai's procurement of the SSL certificate. This includes specification of the Common Name.

2. As part of setup, Akamai procures an SSL certificate on the customer's behalf for the site's Common Name.

3. Upon receiving a request, an SSL handshake with the client begins, presenting the client with the corresponding SSL certificate (as obtained by Akamai).

4. The Akamai edge server checks that the request matches the Common Name requested.

5. Maintaining the SSL session with the client, the edge server connects to the customer origin server.

6. In the ensuing SSL handshake, the origin site presents a server certificate to the edge server.

7. The origin certificate is checked to be sure that it hasn't expired and that it is signed by an authorized Certificate Authority (CA). In this certificate, the Common Name could be the same as the Common Name in the certificate Akamai provided to the client. In actual practice, however, Akamai recommends that the certificate Common Name be different.

8. If the handshake is successful, the connection opens and the client's request is sent over HTTPS to the origin.

9. Once SSL sessions have been established with both the origin and the client, the edge server can forward requests to the origin, and fetch content from the origin to deliver to the end-user.

Data Flow

Edge servers communicate securely with both end-users and customer origin servers. The data flow for transactions involving cardholder data is as follows:

End-User to Customer Origin Server:

1. An enduser submits PII through client software on their computer.

2. That data is encrypted using SSL and transmitted to an Akamai edge server.

3. The edge server decrypts the data, re-encrypts it with the origin server session key, and sends the PII to the origin server.

Customer Origin Server to End-User:

1. Based on an end-user request, a customer origin server responds with encrypted PII data to an Akamai server.

2. The Akamai server receives the data, decrypts it, re-encrypts it with the end-user session key, and then sends the encrypted data to the end-user.

3. The end-user's client software receives the PII data and decrypts it.

- Note: Data is always encrypted as it traverses network links

Authentication

The Akamai software library, used for communication on a number of ports, provides two authentication mechanisms:

- Authentication via a cryptographic protocol that requires properly encrypted data to flow between client and server in order to establish a connection.

- Protection against packet replay attacks. If the time skew on packets exchanged between client and server is more than 1 minute, then the connection is terminated.

Configuration Management

Akamai Secure Content Delivery Network edge servers sit on the public Internet and are configured from the same set of restrictive and hardened software and configuration information as those listed above. These edge servers are designed to function as bastion hosts, obviating the need for enclaving the systems behind a separate firewall. The systems are hardened to withstand various types of attack, including different denial-of-service attacks and other known vulnerabilities. In the Secure Content Delivery Network:

Software changes are executed via automated processes, eliminating the need for most human intervention.

Each machine is configured from the same set of software and configuration information using the NOCC's proprietary systems; this ensures uniform deployment across all servers.

Akamai's deployed network functions in an autonomous mode without users logging into the servers to conduct routine system administration.

Access is only granted for forensic and maintenance purposes.

- Administrative logins are restricted to trained and authorized Akamai employees.

- Remote administrative access is only available via cryptographically secure connections and all electronic access to Akamai servers is logged. To further limit access, read-only views and limited diagnostic tools are provided to Akamai personnel performing system diagnostics and analysis, eliminating the need for administrative access to accomplish these functions.

- Akamai's vulnerability management process is designed to ensure that vulnerabilities are quickly identified and resolved, and remediation is rolled into all subsequent releases.

- Akamai's operational controls are designed to ensure that new application ports and services are properly registered and reviewed as part of the design process.