
Question

[Steve Pisani](#) · May 25, 2016

Web applications, and architecture/security related questions

Hi,

Assume an architecture where an ECP Database Server is connected to by one or more ECP Application Servers inside a firewall. The application server hosts the web application that web users connect to.

The Web servers are outside the firewall, and, (using the CSP gateway/server mechanism) issue requests over the SuperServer port and into the application server.

I know that the traffic between the Web Server and the ECP application server can be encrypted using HTTPS, and access to the CSPServer on the Application server is username/password secured.

Q1: In order to bolster security, is it possible for the SuperServer port connection between the AP Server and the Web Server to only be initiated by the Application Server ?

In this model, we're assuming only the Superserver port would be opened on the firewall, CSPGateway Service would be defined to allow only Web Servers IP's sitting outside the firewall, or, IP addresses within the firewall (for admin purposes). All other Services that use the SuperServer port (object bindings, etc) would be restricted to only IP Addresses within the firewall. Given this configuration, the next question would be:

Q2: With the Web Server outside the firewall having only CSP Gateway access into the Application server, other than disabling all non-essential Web Applications, and securing Web applications with authentication/authorisation, are there certain best-practices within CSP or ZEN development that should be followed in order to avoid malicious injection of code by a hacker ?

Thanks -

Steve

[#Security](#) [#Frontend](#) [#Caché](#)

Source

URL: <https://community.intersystems.com/post/web-applications-and-architecturesecurity-related-questions>