Hosting multiple SSL Certificates on a single IP

Solving the IPv4 shortage dilemma

FULL COMPATIBILITY

When it comes to SSL security, hosting companies are increasingly facing issues related to IP addresses scarcity. Today every digital certificate used to provide an SSL connection on a webserver needs a dedicated IP address, making it difficult for hosting companies to respond to increasing demand for security.

GlobalSign has developed a solution to address hosting companies' operational limitations and to let them run multiple certificates on a single IP address, at no detriment to browser and operating system compatibility.

Host Headers

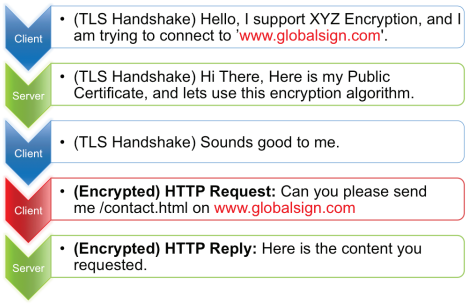
To address the current concern of shortage of IPv4 addresses, most websites have been configured as name-based virtual hosts for years. When several websites share the same IP number, the server will select the website to display based on the name provided in the Host Header.

Unfortunately this doesn't allow for SSL security as the SSL handshake happens before the client makes the first HTTP request which includes the host header.

The role of Server Name Indication

Server Name Indication (SNI), an extension to the TLS protocol, has been available since 2003 for this purpose. This means the hostname of the server is included in the SSL handshake to give the server the possibility to select the corresponding SSL Certificate for the website.

In this case the workflow is as follows:



However the adoption of the extension has been very slow, and a number of systems do not support it by default, such as:

- Internet Explorer (any version) on Windows XP
- Internet Explorer 6 or earlier
- Safari on Windows XP
- BlackBerry Browser
- Windows Mobile up to 6.5
- Android default browser on Android 2.x

(see *http://en.wikipedia.org/wiki/Server_Name_Indication* for the full list).

In public environments, using SNI alone would mean cutting access to a large number of potential site visitors as around 15% of systems (as of January 2013) are incompatible with SNI.

The true solution

By coupling the Server Name Indication technology with SSL Certificates and a CloudSSL Certificate from GlobalSign, multiple certificates can now be hosted on a single IP without losing potential visitors that might lack SNI support.

GlobalSign SSL Certificates can be installed on several name-based virtual hosts as per any SNI-based https website. Each website has its own certificate, allowing for even the highest levels of security (such as Extended Validation Certificates).

GlobalSign will then provide a free fall-back CloudSSL certificate for legacy configurations, enabling the 15% of visitors that do not have SNI compatibility to access the secure websites on that IP address. The CloudSSL Certificate will hold the information of the server administra tor in the subject, and a Subject Alternative Name for each SSL-secured website on the IP number.

This process can be fully automated with GlobalSign's unique application. After a one time configuration, the CloudSSL is automatically created, installed, validated and updated as new websites need to be added or removed. The application is already available for all Apache and NGINX webservers, as well as solutions for custom deployments.

Key Benefits

- **Tackle the IP shortage dilemma -** Host multiple SSL Certificates on a single IP
- **Fully automated process:** One time configuration, independently of control panel
- **Full compatibility:** Including legacy configurations that do not support standard SNI implementations
- **Easy to update:** No DNS changes required
- **Ensure maximum revenues -** Remove barriers to mass deployment of SSL security

Available on:

NGINX Apache

...and custom solutions

For more information about the GlobalSign solutions, please call our specialists at: 1-603-570-7060 or Visit www.globalsign.com for more information.