



Spacenet SSL Acceleration Over VSAT Networks

This document contains information proprietary to Spacenet Inc. (Spacenet). It may not be reproduced in whole or in part without the written consent of Spacenet. The disclosure by Spacenet of information contained herein does not constitute any license or authorization to use or disclose the information, ideas, or concepts presented.

Background

VSAT networks historically have employed methods of acceleration to overcome the effects of latency on protocol performance and user experience. Gilat has developed acceleration techniques to mitigate the effects of satellite latency at the transport and application layers and embedded them within our VSAT network products. TCP Acceleration improves raw throughput, while Internet Page Accelerator dramatically reduces the time to load Web pages to a user's browser. As with all acceleration techniques, TCP Acceleration and Internet Page Accelerator (IPA) examine the appropriate protocol header information and act upon that information in order to perform the acceleration.

SSL stands for Secure Socket Layer and runs above TCP/IP to allow for secure, authenticated data transfer between two computers. It is a way to create an encrypted channel for communication between a browser and a web server that prevents the eavesdropping of data contents passing over a public infrastructure. This is essential when sensitive information such as credit card numbers or company sensitive information is being sent. The main goals of SSL is first, encryption and second, authentication.

The encryption and authentication performed by SSL prevents web users from realizing the improved performance web acceleration techniques, such as IPA, offers. SSL encrypts not only the user data, but also the HTTP protocol information used by IPA to accelerate web page loading. In addition, the encryption key and authentication exchanges require from four to eight round trips between the browser and the web server per object on each page, further degrading the user experience. See Figure 1 for an example of the SSL handshakes required to request a single object on a web page. Given that most web pages currently contain between 10 and 100 objects, the time to load secure web pages to a browser over a satellite link is generally unacceptable.

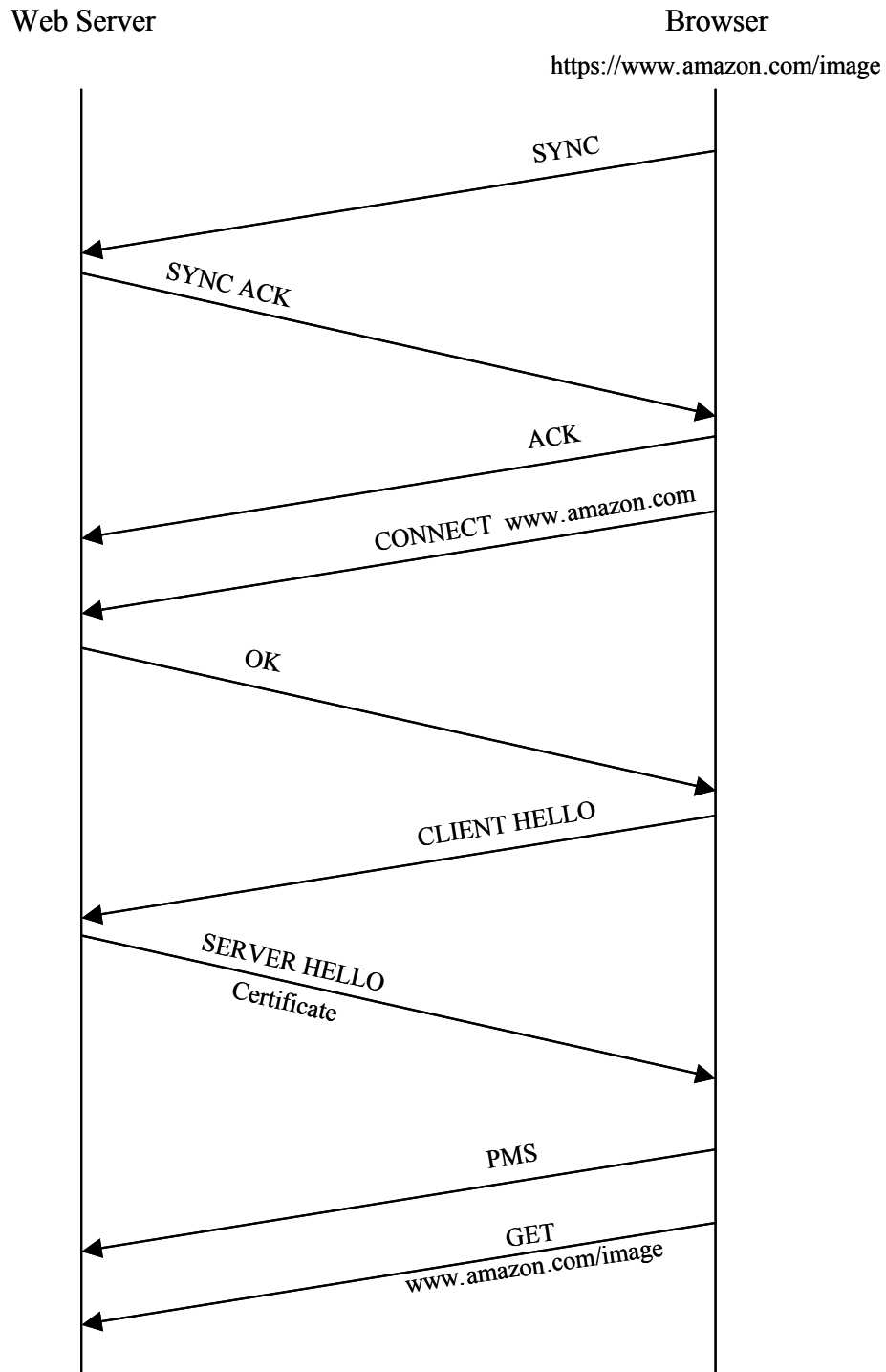


Figure 1, Sample SSL Protocol Diagram

SSL-IPA Overview

In order to bring the user experience when browsing secure web sites to the superior level of standard web sites accessed using IPA, Gilat has developed the SSL-IPA. SSL-IPA is an optional version of the standard IPA that allows for the establishment of encryption and authentication between the Remote Page Accelerator (RPA) and the user's browser and the Hub Page Accelerator (HPA) and the web server, thereby allowing IPA to interpret the HTTP information within and perform its standard acceleration techniques. The RPA is a WIN32 application installed at each remote location in the VSAT network. It can run on the PC with the browser, or may be installed on a dedicated PC providing proxy services to all browsers in a remote location. Figure 2 shows a simplified block diagram of these configurations. Data between the RPA and HPA is secured by the VSAT network and by SSL between the VSAT network and the web servers/browsers.

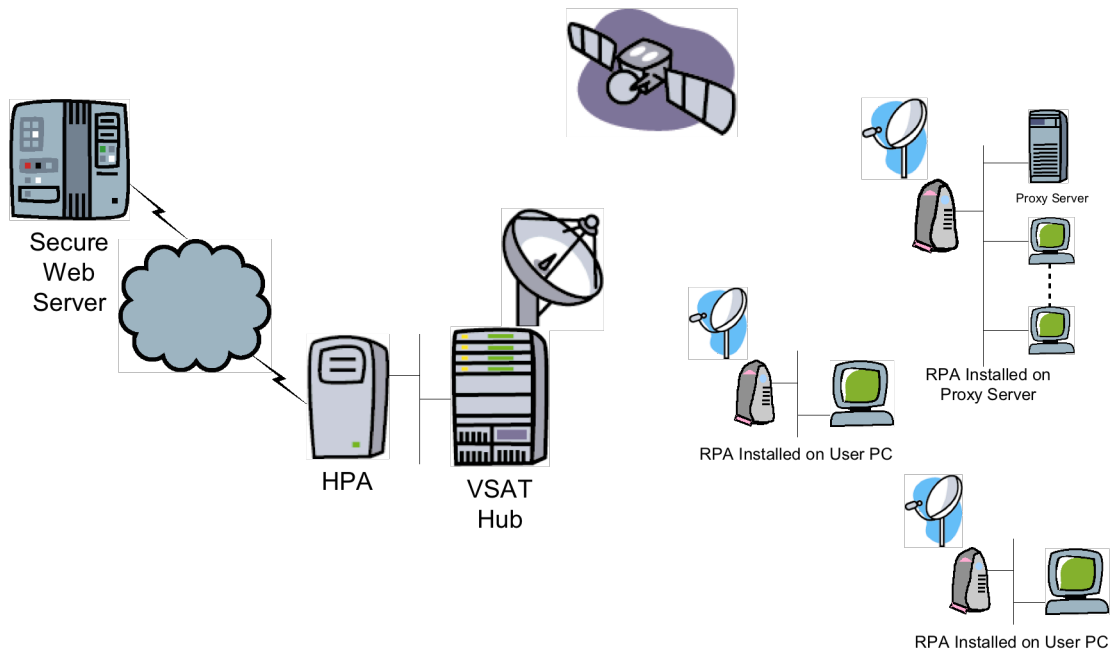


Figure 2, SSL-IPA Block Diagram (RPA on PC or Proxy Server)

SSL Sessions through SSL-IPA

As previously mentioned, the RPA is a WIN32 application installed at each remote location, either on each PC, or on a central PC at the remote sites. In either case, the browsers are configured to use the RPA as their proxy server for HTTP and Secure Web sites. Part of the RPA installation is to configure the browser to recognize the RPA SSL Certificate as a trusted certificate issued by a recognized Certificate Authority. The RPA SSL Certificate is what is known as a Self Signed Certificate Authority in SSL standards.

When browsing secure Web sites through the SSL-IPA, the SSL sessions are established and maintained between the RPA and the browser(s); and between the HPA and the Web server(s). To the browser, the RPA functions as the server for the SSL authentication, key exchanges and encryption. To the Web server, the HPA functions as the browser for the same. Security of the data across the Internet is ensured by the SSL session between the Web server and the HPA. Data across the satellite is secure from interception by the multiple layers of security inherent in the Skystar products.

Refer to Figure 3 for an example of an SSL handshake sequence to load one object on a web page when utilizing SSL-IPA. When a user whose browser is configured to use the SSL-RPA as its proxy requests an object from a secure site, the browser sends a CONNECT message. This is intercepted by the RPA and the RPA returns an OK response. The browser then initiates the SSL session by sending a HELLO message. The SSL session initiation continues between the browser and the RPA. The RPA has its own public and private keys, along with its certificate generator, for exchanges with the local browser. Once the session is established, the browser sends its GET request to begin loading the web page.

At the HPA/Web server side of the connection, the HPA initiates the SSL handshaking and connection establishment with the Web server on the browser's behalf. When the HPA validates the certificate as valid, it then forwards the GET request to the Web server. Should the Web server return an invalid certificate, the HPA will prompt the user through the RPA to select whether or not to continue. When validation is complete, the web page loads through the normal IPA mechanisms.

In this example, the number of hops over the satellite network is reduced from four without SSL-IPA to one. Since the exchanges are occurring either locally or over low latency links, the total time to get the object is dramatically reduced.

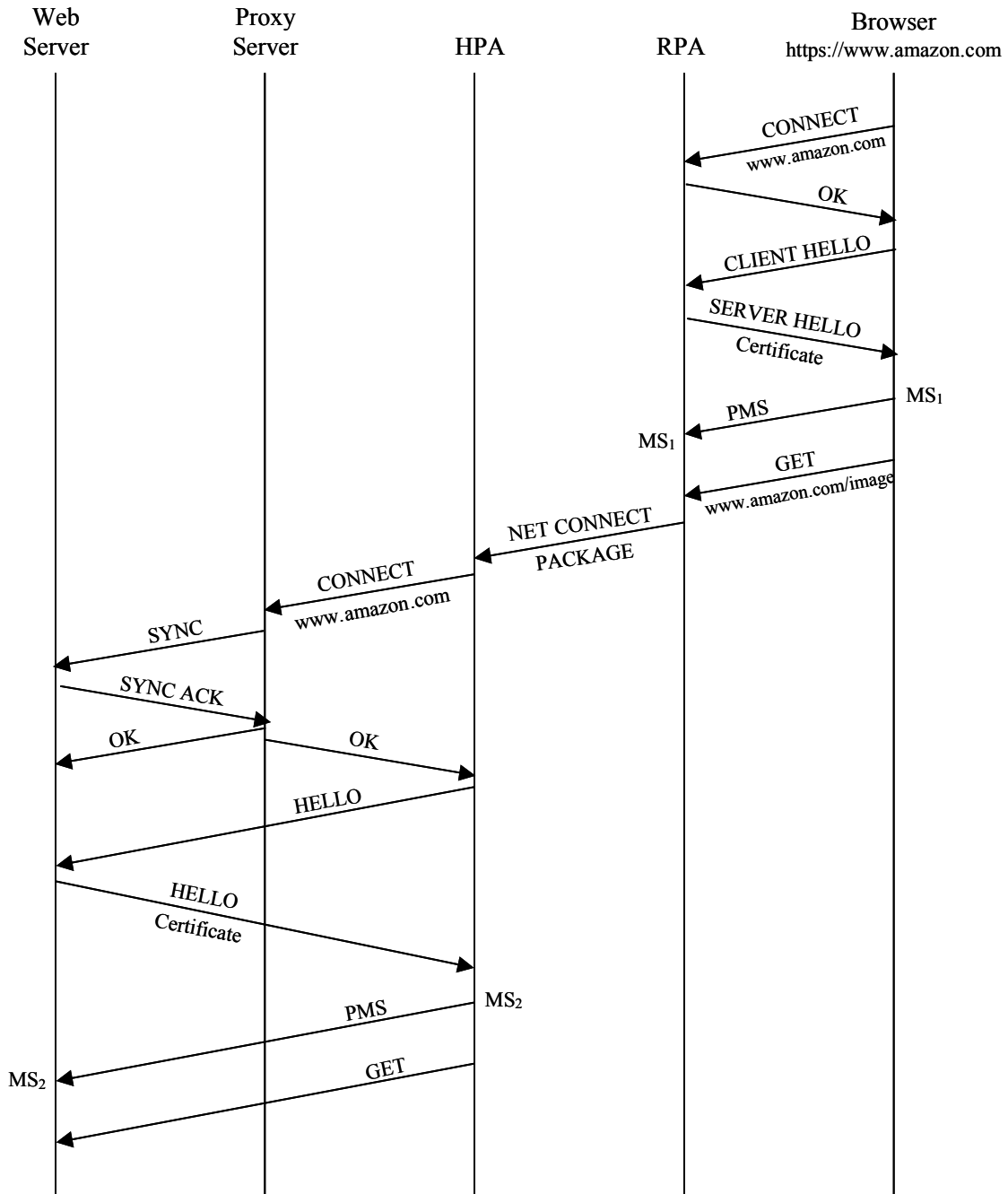


Figure 3, SSL-IPA Ladder Diagram

Conclusion

As companies expand their leverage of the Internet, the need to secure their data across public infrastructures becomes increasingly important. VSAT networks are able to provide broadband coverage to the end users. The latency inherent in a satellite network poses challenges to service providers and IT departments needing to deliver applications to a geographically dispersed user base without compromising the user experience. Gilat's SSL-IPA allows IT departments to deliver applications securely without needing to sacrifice user experience or to modify the method of application delivery.

Glossary of Acronyms

HPA	Hub Page Accelerator
IPA	Internet Page Accelerator
MS	Master Secret Key
PMS	Pre-Master Secret Key
RPA	Remote Page Accelerator
SSL	Secure Socket Layer
VSAT	Very Small Aperture Terminal