“Always-on SSL” – which enables SSL encryption for all Web pages as well as more robust SSL encryption – is becoming increasingly popular. The trend to keep enhancing existing security levels rapidly ramps up the processing load on servers. Potential solutions are presented in this article.

The Internet has quickly become an indispensable part of our social infrastructure, but at the same time, there are innumerable security threats associated with websites, and they become ever more advanced and complex with each passing year.

For example, threats like “man-in-the-middle (MITM) attacks” that steal personal data by capturing communications packets transmitted over Wi-Fi have become much more common due to the widespread use of smartphones. In order to better protect users, an increasing number of websites have recently adopted SSL encryption, or so-called ‘always-on SSL’, in addition to that applied to authentication and settlement pages.

SSL encryption itself has also been reinforced to better withstand the more advanced methods of attack that are now employed. Until recently, encryption using 1024-bit keys was standard, but 2048-bit keys have now become prevalent. If even stronger security is demanded, encryption with 4096-bit keys has been used in some of the latest cases. In fact, use of 1024-bit encryption was rendered obsolete at the end of 2010 by the National Institute of Standards and Technology (NIST), and all major Web browsers already support 4096-bit encryption.

While this trend affords many advantages to website users, it also presents a major hurdle for Web server operators. This is because as SSL encryption is enhanced, the processing load for encryption and decryption becomes correspondingly more intense. As a general rule, any increase in the key length from 1024 to 2048-bit keys requires four to seven times more CPU processing power.

Moreover, once this encryption/decryption processing is applied to all Web pages, the load on the Web server becomes extremely large. The adoption of an “SSL offload” method that enables an Application Delivery Controller (ADC) to process SSL encryption/decryption has recently been promoted as a solution to these issues. Among these, ADC products noteworthy for the attention they are attracting are A10 Networks’ “AX Series”.

The AX Series is notable for its ability to quickly perform the encryption/decryption process even when the encryption method involves long keys thanks to the combination of its proprietary 64-bit OS “ACOS”, with dedicated hardware.

Dedicated hardware known as an “SSL Acceleration Card” can be added to high-end models to boost the SSL offload speed. For example, the performance of the top model, “AX 5630”, in the case of 2048-bit encryption is just two percent below that achieved for 1024-bit encryption.

ADCs that enable 2048-bit encryption processing with almost the same performance levels as 1024-bit are rare anywhere in the industry. Additionally, the realization of always-on SSL and the shift to 4096-bit encryption in the future can easily be handled because many more SSL connections can quickly be handled even with the same encryption method.

The AX Series enables 2048-bit encryption to be processed at the same speed as 1024-bit encryption.

Furthermore, adoption of the AX Series facilitates swift realization of a process known as “SSL Intercept”, which involves the decoding of encrypted communications, and re-encryption and transmission after verifying that no malware has been introduced via the Internet and that no confidential information has been syphoned off via the LAN, using optional security products.