The New Certificate 2048 My Performance

Peter Silva, 2010-19-10

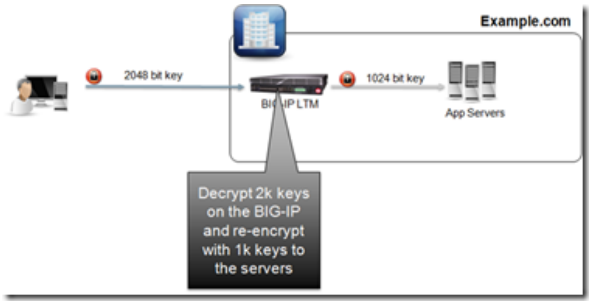
SSL is a cryptographic protocol used to secure communications over the internet. SSL ensures secure end-to-end transmission and is implemented in every Web browser. It can also be used to secure email, instant messaging and VoIP sessions. The encryption and decryption of SSL is computationally intensive and can put a strain on server resources like CPU. Currently, most server SSL Certificates are 1024-bit key length and the National Institute of Standards and Technology (NIST) is recommending a transition to 2048-bit key lengths by Jan 1st 2011.

SSL and its brethren, TLS (Transport Layer Security) provide the security and encryption necessary for secure communications over the internet, and particularly for creating an encrypted link between the browser and web server. You will see 'https' in your browser address bar when visiting a site that is SSL enabled. The strength of SSL is tied to the size of the Public Key Infrastructure (PKI) key. Key length or key size (1024 bit, 2048 bit, 4092 bit) is measured in bits and typically used to indicate the strength of the encryption algorithm; the longer the key length, the harder it is decode. In order to enable an SSL connection, the server needs to have a digital certificate installed. If you have multiple servers, each requiring SSL, then each server must have a digital certificate.

Transactions handled over SSL can require substantial computational power to establish the connection (handshake) and then to encrypt and decrypt the transferred data. If you need the same performance as non-secured data, then additional computing power (CPU) is needed. SSL processing can be up to 5 times more computationally expensive than clear text to have the same level of performance, ***no matter which vendor is providing the hardware***. This can have significant, detrimental ramifications to server performance. SSL Offload takes much of that computing burden off the servers and places it on dedicated SSL hardware. SSL offload allows organizations to migrate 100% of their communications to SSL for greater security, consolidation of certificates, centralized management, and reduction of cost and allows for selective content encryption & encrypted cookies along with the ability to inspect and modify encrypted traffic. SSL offloading can relieve the Web server of the processing burden of encrypting and/or decrypting traffic sent via SSL.

Customers, vendors and the industry as a whole will soon face the challenge of what to do regarding their SSL strategy. Those who have valid 1024-bit certificates need to understand the ramifications of the switch and that next time they go to renew their certificates, they will be forced to buy 2048-bit certificates. This will drastically affect their SSL capacity on both the servers and the load balancer. There is a significant increase in needed computational power going from 1024-bit to 2048-bit and an exponential drop off in performance when doubling key sizes regardless of the platform or vendor. Most CAs, like Entrust have already stopped issuing 1024-bit certificates, and Verisign will stop doing so in 4-5 months. Since many certificate vendors are now only issuing 2048-bit certificates, customers might not understand the potential SSL performance capacity. The overall performance impact of 2048-bit keys on the servers if you don't offload will increase significantly. This can be a challenge when you have hundreds of servers providing content.

Existing certificates issued with 1024-bit encryption will not stop working. If you still have valid certificates but need to ensure you are delivering 2048-bit certificates to users (or due to regulatory requirements), one option, as mentioned in Lori's blog, is to install the 2048-bit certificate on your BIG-IP LTM for the off-load performance capabilities and then use your existing 1024-bit keys from BIG-IP LTM to the back-end server farm. Simply import the server certificates directly into BIG-IP. This means that the SSL Certificates that would normally go on each server can be centrally stored and managed by LTM, thereby reducing the cost of the certificates needed as well as the cost for any specialized server software/hardware required. This keeps the load off the servers, potentially eliminating any performance issues and allows you to stay current with NIST guidelines while still providing an end to end SSL connection for your web applications. This is a huge advantage over commodity hardware with no SSL offload capabilities. BIG-IP LTM has specialized SSL chips which are dedicated and optimized for SSL encryption and decryption. These chips provide the ability to maintain performance levels even at longer key lengths, whereas in commodity hardware the computational load of SSL decreases the overall system performance impacting user experience and other server tasks.



The F5 SSL Acceleration Module removes all the bottlenecks for secure, wire-speed processing, including concurrent users, bulk throughput, and new transactions per second along with supporting certificates up to 4092-bits. The fully loaded F5 VIPRION chassis is the most powerful SSL-offloading engine on the market today and, along with the BIG-IP LTM Virtual Edition (VE), provides a powerful solution to the SSL challenge. By front-ending BIG-IP VE farms with a VIPRION, you can assign load balancing or SSL offloading to a dedicated ADC. The same approach can remedy access to legacy systems that might not support 2048-bit certificates or cannot be upgraded due to business restrictions or other rationale. By deploying an F5 BIG-IP device with 2048k certificate in front of the legacy systems, back-end encryption can be accomplished using existing 1024-bit certificates. F5 does support 4096-bit keys, future-proofing support for longer keys down the road and offers backwards and forwards compatibility but unless there is a strong business case, 2048-bit keys are recommended for optimal performance and protection.

ps

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com