Increase SSL Offload Performance with the BIG-IP Platforms

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. The encryption and decryption of SSL is computationally intensive and can put a strain on server resources like CPU. F5® BIG-IP® Application Delivery Controllers offer SSL offloading, providing relief from the processing burden of encrypting and decrypting traffic sent via SSL.

SSL Processing and Offload

SSL offload helps organizations migrate 100 percent of their communications to SSL for greater security, consolidation of certificates, centralized management, and reduction of cost. In addition, SSL offload allows for selective content encryption and encrypted cookies along with the ability to inspect and modify encrypted traffic. 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 encrypt and decrypt the transferred data. SSL processing can cost five times more than clear text for the same level of performance, no matter which vendor provides 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. This reduces the needed power significantly and puts less strain on the servers.

The industry as a whole will soon face the challenge of what to do regarding their SSL strategy. 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 January 1, 2011. Those who have 1024-bit certificates need to understand the ramifications of the switch. At renewal, everyone will be required to buy 2048-bit certificates. This will drastically affect SSL capacity on both the servers and the load balancer. There is a significant increase in needed 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.

Existing certificates issued with 1024-bit encryption will not stop working. If you still have valid certificates but need to ensure you can deliver 2048-bit certificates, one option is to install 2048-bit certificate on a BIG-IP® Local Traffic Manager™ (LTM). By directly importing certificates that are normally on each server, administrators can centrally store and manage certificates with BIG-IP LTM. This reduces the cost of the needed certificates as well as the cost for any specialized server software or hardware required. The load stays off the servers, eliminating performance issues and providing an end-to-end SSL connection that complies with NIST guidelines. BIG-IP LTM has specialized SSL chips that are optimized for SSL encryption and decryption. These chips help maintain performance levels even at longer key lengths, whereas in commodity hardware without SSL hardware, the computational load of SSL decreases the overall system performance affecting user experience.

Key features

- **BIG-IP Flexibility**—Uses 2048-bit keys, but retains 1024-bit keys to back-end servers
- **Device Inventory and Control**—Keeps critical device and certificate information in a central location
- **Centralized SSL Management**—Imports server certificates directly into BIG-IP devices and streamlines BIG-IP® Enterprise Manager™ certificate management
- **Selective Content Encryption**—Holistically, partially, or conditionally encrypts data without requiring changes to application code
- **Specialized Hardware**—Offers SSL offload with specially designed 8950S platform

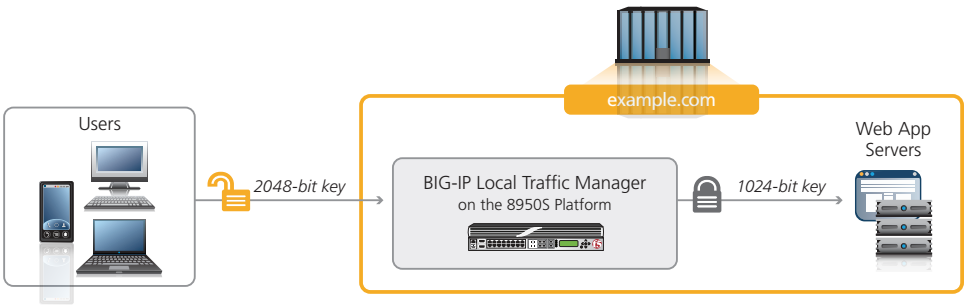
Key benefits

- **Increase Security**—Allows organizations to migrate 100 percent of their communications to SSL for greater security
- **Certificate Consolidation**—Consolidates SSL certificates for centralized management on one BIG-IP device
- **Increased SSL Performance**—Boosts application security and performance without adding more servers to the infrastructure
- **Reduce Cost**—Eliminates the need to buy and install SSL-capable server software on every server
- **Granular Control**—Inspects and modify encrypted traffic to take action prior to re-encryption or delivery

Solution

F5 SSL offload and acceleration removes all the bottlenecks—including concurrent users, bulk throughput, and new transactions per second along with supporting certificates up to 4096-bits—for secure, wire-speed processing. The 8950S platform is specially designed to handle high throughput and bulk SSL transactions, doubling the performance of the 8900 platform, and a fully loaded F5 VIPRION® chassis is the most powerful SSL-offloading engine on the market today. Along with the F5 BIG-IP LTM Virtual Edition (VE), these platforms provide a powerful solution to the SSL challenge.

By front-ending BIG-IP LTM VE farms with a VIPRION device, you can assign load balancing or SSL offloading to a dedicated unit and assign BIG-IP LTM VE to do the particular task of load balancing for the server farms or even the SSL offload itself. The same approach can remedy access to legacy systems that might not support 2048-bit certificates or cannot be upgraded due to business restrictions. By deploying an F5 BIG-IP device with 2048-bit certificate in front of the legacy systems, back-end encryption can be accomplished using existing 1024-bit certificate. F5 devices support 4096-bit keys and provide support for longer keys down the road.



Offload SSL processing to BIG-IP LTM

Learn more

For more information about BIG-IP SSL acceleration solutions, please see the following resources or use the search function on f5.com.

BIG-IP product pages

BIG-IP Hardware

BIG-IP Local Traffic Manager

F5 SSL Acceleration

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.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

CS18-00006 0611