F5 Synthesis: Hybrid SSL Offload

Lori MacVittie, 2014-01-10

#SSL #webperf #infosec

Now your services can take advantage of hardware acceleration even when they're deployed on virtual machines

Way back in the day, when SSL offloading was young and relatively new, there were a variety of hardware, software and even architecture that arose to defeat the security penalty imposed by the requisite cryptographic functionality.

Most commonly, we'd slap a PCI-card into a server, muck with the web server configuration (to load some shared objects) and voila! Instant performance boost via hardware acceleration. Later, an architectural approach that leveraged a network-based offload capability was introduced. This meant configuring an SSL offload appliance in a side (or one) arm configuration (common for caches and even load balancers back then) in which SSL traffic was routed to the offload appliance and decrypted before being sent on to the web or app server. You added some latency in the hairpin (or trombone, if you prefer) but that was always more than offset by the improvement of ***not*** letting the web server try to decrypt that data in the first place.

We've come a long way since then and most often these days you'll find an application delivery controller (ADC) or an app proxy serving duty as cryptographic master of the application. Most ADCs are still far more efficient at handling SSL/TLS traffic because they've benefitted from Moore's Law in two places: the core system and the SSL acceleration hardware (which takes advantage of CPUs, too, in addition to custom hardware).

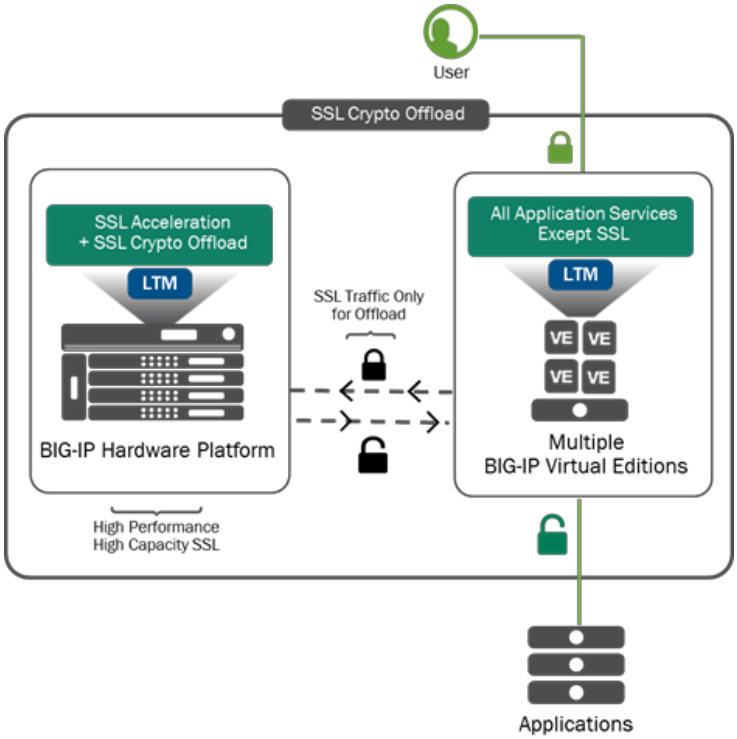
Now comes the advent of the next generation of application delivery architectures which, necessarily, rely on a fabric-based approach and incorporate virtual appliances as well as traditional hardware. Services deployed on the hardware of course benefit from the availability of specialized SSL acceleration but the virtual appliances? Not so much.

We (as in the corporate We) didn't like that much at all, especially given trends toward greater key lengths and the forthcoming HTTP 2.0 specification which, yes, requires SSL/TLS. That means a lot more apps are going to need SSL - but they aren't going to want the associated performance penalty that comes with it running on software. They may not be as important, but they aren't expendable. That's true whether the web server natively handles SSL or you move it off to a virtual ADC within the services fabric. All apps are important, of course, but we know that some are more important than others and thus are afforded the benefits of services deployed on faster performing hardware while others are relegated to virtual machines.

We take our commitment with Synthesis to leave no application behind seriously and thus have introduced the industry's first hybrid SSL offload capability.

Hybrid SSL Offload

Hybrid SSL Offload was made available with the release of BIG-IP 11.6 and enables virtual editions of BIG-IP as well as less capable and legacy BIG-IP appliances and devices to harness the power of hardware to improve app performance through cryptographic acceleration. This has the added benefit of freeing up resources on virtual appliances to improve the overall performance and capacity of app services deployed on that virtual edition.



In a nutshell, user requests are sent to the appropriate virtual ADC instance, which hosts all app services for an app *except* SSL. SSL is offloaded to a designated service running on a hardware platform that can take advantage of its targeted hardware acceleration.

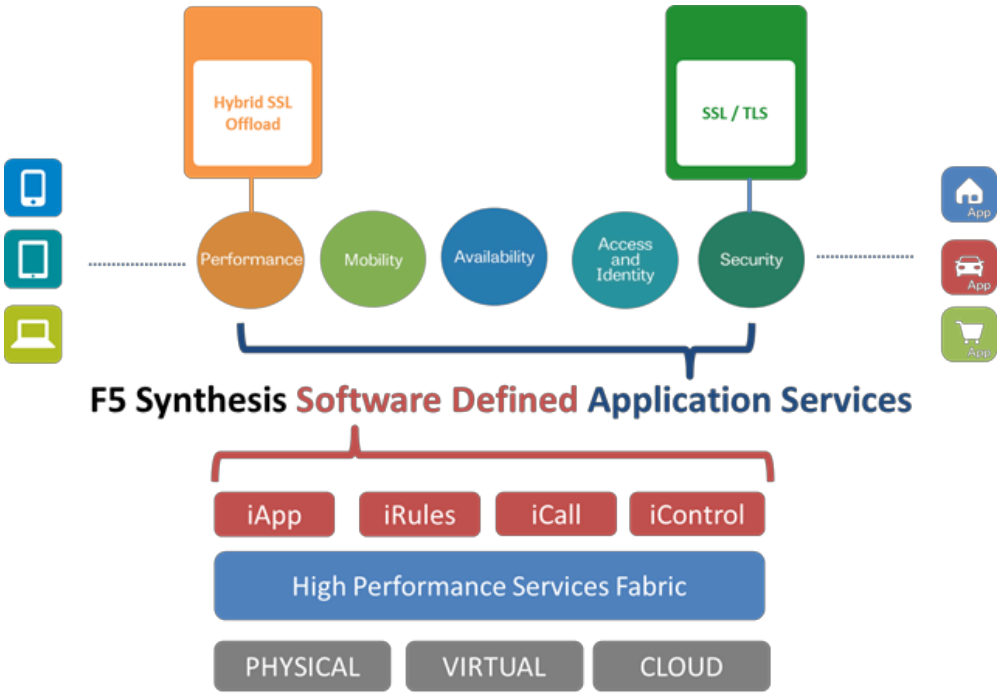
Using hybrid SSL offload within the Synthesis service fabric allows organizations to:

•Achieve the maximum SSL performance of a virtual license

•Free up Virtual Edition CPU utilization for other application services

All together this means better app performance and capacity for services deployed on virtual editions.

All applications need services and deserve optimal performance, even those that might otherwise by designated as "red shirt" apps by IT. F5 Synthesis continues to leave no application behind by ensuring every application has access to the services it needs, even when it means collaborating across device types.



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

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113