Makani SSL Acceleration

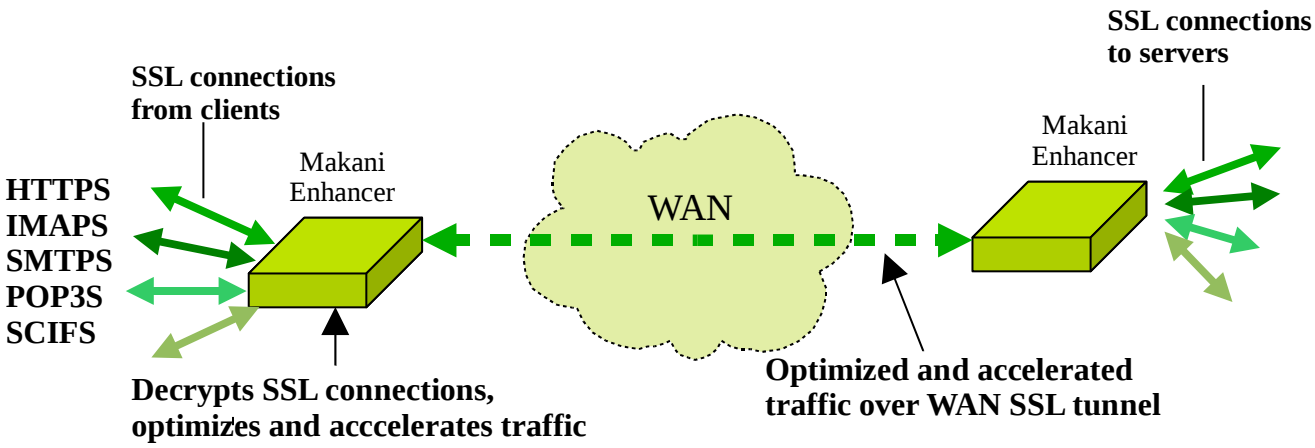
As data security has become a more important concern for organizations, many of these organizations are adopting policies that mandate migration to SSL transports to ensure that data in flight is always protected. Unfortunately, many of these organizations could do very little to truly optimize and accelerate the performance of these encrypted applications while still maintaining the security of the data.

SSL Acceleration: The Challenge

Existing solutions to symmetric secure traffic acceleration generally introduce security issues, use inferior acceleration techniques, or both. The primary difficulty in an encryption system like SSL is typically protecting the private key information. This challenge of key management is that it's not very sensible to make a symmetric acceleration device support SSL by simply putting the origin server's private key information onto every device. In organizations with a large number of branches, there would be a correspondingly large increase in the chance of *exposure* of the private key of each server whose traffic should be optimized.

Transparent SSL Acceleration

Makani appliances are designed to transparently optimize and accelerate traffic that are encrypted using **SSL**. Makani appliances do so by applying all of the same set of optimizations they apply to unencrypted traffic over the WAN. Makani accomplishes this while maintaining complete "end-to-end" security and maintaining the trust model that enterprises require. The approach from Makani allows end-to-end secure traffic and secure WAN traffic optimization and acceleration that offer LAN-like performance over the WAN. Each client uses unchanged server addresses and each server uses unchanged client addresses; no application changes or explicit proxy configuration is required.



Makani's transparent SSL traffic optimization and acceleration

In an ordinary SSL handshake, the client and server first establish identity using public-key cryptography, then negotiate a symmetric “session” key to be used for the actual data transfer. Using the Makani platform, the initial SSL message exchanges take place between the client and the client-side Makani appliance, which initiates a connection with the server-side Makani appliance. The server-side Makani appliance then sets up a SSL connection to the server to satisfy the client request. The effect of this is that the client's SSL connection logically terminates at the server, but physically terminates at the client-side Makani appliance. The approach is completely transparent to the user or application.

Note that SSL is a general-purpose technology that can secure a variety of application protocols. In the same way, Makani’s SSL acceleration is designed as an application-independent technology. Although the most common use of SSL acceleration is for HTTPS, however, all of the WAN optimization mechanisms can be used on any SSL traffic meant for optimization.

Conclusion

Makani's transparent SSL optimization and acceleration gives enterprises new, better choices in the security vs acceleration tradeoff. With Makani's approach to end-to-end SSL traffic acceleration, enterprises may choose to mitigate more of their applications to SSL-encrypted protocols to give them the data security they are looking for. With Makani, they can be assured that they can still access the information they need at LAN-like speeds, no matter where in the world their office or data center is located.

Makani offers high-performance, easy-to-use and technically innovative solutions for next-generation wide-area networked data services. Makani Enhancers™ are deployed for wide-area data acceleration and optimization. Makani Mobilizer™ appliances are deployed in the customer's network for blazing-speed data access over a wide-range of access networks. Founded in 2006, Makani is headquartered in San Francisco with regional offices all over the world.