

Accelerate Encrypted SSL/TLS Traffic Across Complex Defense Network Environments

The Department of Defense operates some of the most dynamic and dispersed network environments in the world, all faced with a herculean task of meeting the ever-growing demands of mission-critical users.

These demands placed on DOD networks from the explosive growth in Cloud and SaaS adoption, coupled with a massive increase in remote work, has not only made DOD networks more distributed and complex, but often outpaced available capacity. The result is often crippling latency, reduced application performance and poor end-user experiences.

To compound these issues, nearly 85% of DOD's network traffic is encrypted using SSL/TLS protocols, presenting unique challenges to unlock greater capacity. In the past, to optimize and accelerate encrypted traffic and applications involved lengthy security conversations, logistical hurdles, sharing or copying hundreds of certificates and keys, perceived network security risks, and in the end, was often deemed too risky and difficult a process for agencies.

Until Now

As encrypted traffic started overtaking public sector networks, Riverbed began reengineering its optimization and acceleration solutions to meet the new norm of SSL/TLS encryption.

Riverbed's enhanced SteelHead WAN Optimization and Client Accelerator solutions simplify the authentication process of SSL/TLS traffic. Client Accelerator now functions like a Hardware Security Module (HSM) by granting access to the "session" key, which is unique and randomly generated, for each encrypted communication session.

This novel approach to authentication bypasses the traditional SSL/TLS "handshake" that requires public and private keys and certificates and instead allows encrypted network communications between authorized users and applications within the SteelHead optimization fabric. No sensitive keys or credentials are ever exchanged or exposed.

Once a SSL/TLS session is authenticated and an encrypted connection is established, Defense agencies can easily unlock network capacity and improve application performance to meet the ever-growing demands of global users.



Figure 1.
Riverbed's enhanced
SSL/TLS network
acceleration solutions.

Breakthrough Performance and Speed for Defense Encrypted Apps and Traffic:

- Achieve zero-touch SSL/TLS optimization and acceleration
- Unlock critical capacity across any Defense network environment
- Maintain and strengthen network security postures
- Boost the performance of any on-prem or SaaS SSL/TLS applications by up to 10x
- Reduce bandwidth requirements by up to 99%
- Realize true value of IT investments
- Transparently operate with mutual authentication (CAC) and advanced TLS (ECDH, PFS)
- Eliminate certificate management

Reduce bandwidth requirements by up to **99%**

Challenge

One of the Department of Defense's Uniformed Services Branches (USB) operates in bandwidth-challenged remote locations across the world where a "Logistics" application, among other mission-critical applications, had been rendered inaccessible due to extreme latency on the Command's satellite network. Without this application, service technicians could not procure crucial parts needed to repair military assets, resulting in these assets being taken offline and exposing a significant operational vulnerability. Like other Defense agencies, the USB had previously

been reluctant to optimize and accelerate its SSL/TLS traffic due to perceived network security concerns.

Solution

The USB had previously been working with Riverbed to optimize and accelerate its non-encrypted traffic. When evaluating and testing the SSL/TLS-enhanced SteelHead WAN Optimization and Client Accelerator solutions, the USB was easily able to configure and deploy, identify the SSL/TLS application for acceleration, authenticate with the application's "session" key, and establish encrypted network session. Then the USB employed

traditional optimization and acceleration approaches that significantly reduced latency and unlocked network capacity, all while maintaining an encrypted environment.

Benefits

With Riverbed's enhanced SteelHead WAN Optimization and Client Accelerator, the USB was able to optimize and accelerate the SSL/TLS traffic unlocking nearly 3x satellite bandwidth capacity. More importantly, the USB was able to bring its mission-critical logistics application online, secure the parts and supplies needed to repair military assets, and support warfighters in the field.



Riverbed – Empower the Experience

Riverbed is the only company with the collective richness of telemetry from network to app to end user that illuminates and then accelerates every interaction so that users get the flawless digital experience they expect across the entire digital ecosystem. Riverbed offers two industry-leading solution areas – Alluvio by Riverbed, an innovative and differentiated Unified Observability portfolio that unifies data, insights, and actions across IT, so customers can deliver seamless digital experiences; and Riverbed Acceleration, providing fast, agile, secure acceleration of any app over any network to users, whether mobile, remote, or on-prem. Together with our thousands of partners, and market-leading customers across the world, we empower every click, every digital experience. Learn more at riverbed.com.