Wednesday, February 16, 2022
2:10 PM – 2:30 PM
Accelerate Encrypted Network Environments On-Shore or At-Sea for Naval and Marine Corps Mission Success

Marlin McFate
Public Sector CTO
Riverbed/Aternity

Abstract:
The United States Navy and Marine Corps (USN/USMC) operate some of the most dynamic and dispersed network environments in existence and the personnel responsible face a Herculean task ensuring the communications, connectivity and mission readiness of Sailors and Marines at sea, on shore and in the air. To support their missions, the USN/USMC rely on a complex environment of terrestrial, cloud, and satellite (SATCOM) networks. From the Navy/Marine Corps Combined Intranet (NMCI) and OCONUS Navy Enterprise Network (ONE-Net) to the Marine Corps enterprise Network (MCEN) and Networking on the Move (NOTM), the ability to enable a unified computing and networking environment requires delicate management of finite capacity in the face of shifting demands and needs.

As a result of digital transformation and growing Cloud and SaaS adoption, the USN/USMC have seen their networks grow more distributed and complex --- to the point that mission needs can outpace available capacity. To compound these issues, nearly 85% of USN/USMC network traffic is encrypted using SSL/TLS protocols, presenting unique challenges to unlock greater capacity and accelerate networks.

To address these challenges including encrypted traffic and applications, many USN/USMC Commands use Riverbed Technology's SteelHead Network Acceleration Solutions on shore, at sea and on the move, to assist in freeing up desperately needed capacity. However, encrypted traffic can be a double-edged sword. It's critical to ensuring the security and integrity of USN/USMC networks, but it requires the proxying and caching of thousands of sensitive keys and certificates, loading them onto and maintaining in network environments.

As encrypted traffic started overtaking USN/USMC networks, Riverbed reengineered its SteelHead network acceleration solutions to meet the new norm of SSL/TLS encryption and to ensure that USN/USMC could simplify the authentication process of SSL/TLS traffic and unlock greater capacity on their networks. SteelHead 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. Instead, it 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 an SSL/TLS session is authenticated and an encrypted connection is established, USN/USMC network operations teams (NetOps) can quickly unlock network capacity and improve application performance to meet the demands of Sailors and Marines across the globe. In addition, Riverbed's new SteelHead Network Acceleration Solutions are going to be crucial for

the USN/USMC as they evolve to Joint All-Domain Command and Control (JADC2), Zero Trust architectures, and Joint Warfighter Cloud Capability (JWCC) environments, all which heavily rely on the digital services with SSL/TLS encryption.

At West 2022's Innovation Showcase, Riverbed is prepared to demonstrate this new capability and outline how USN/USMC can take advantage of this technological advancement to unlock up to 75% of additional capacity on finite network resources and ensure the mission readiness.