Content and Bandwidth Management (CBM) – Bandwidth Utilization

THE CHALLENGE

In 2014, the Marine Requirements Oversight Council designated the Marine Corps Director, Command, Control, Communications, and Computers (Dir, C4) as the USMC's Bandwidth Manager. Dir, C4 was also tasked to conduct a two-year bandwidth utilization assessment to objectively determine the bandwidth requirements baseline for a "seamless" Marine Corps Enterprise Network that encompassed both garrison and tactical activity stretching "from the foxhole to the flagpole". In September 2015 CSCI was tasked by Dir, C4 to monitor Marine Corps tactical Internet Protocol (IP) bandwidth usage in "relative" tactical environments, document bandwidth usage inefficiencies, and to investigate methods to increase efficient bandwidth usage on tactical networks.

THE STRATEGY

Dir, C4 directed that CSCI use Orion's SolarWinds™ network monitoring software suite as CBM's primary collection and analysis tool. Because of CSCI's familiarity with the Marine Aviation Weapons and Tactics Squadron's bi-annual Weapons and Tactics Instructor (WTI) Course, the two Fiscal Year 2016 WTI courses held in Yuma, Arizona provided the initial venues for data collection. WTI 1-16 (in October 2015) provided the initial tactical network baseline data for a Marine Expeditionary Brigade (MEB)-sized, aviation-centric exercise. Lessons learned from WTI 1-16 were applied to the following collection effort at WTI 2-16 in April 2016.

During WTI 2-16, CSCI established SolarWinds™ Network Performance Manager (NPM) and Network Traffic Analyzer (NTA) instances for data collection. NPM was used to collect and display Simple Network Management Protocol (SNMP) health and status data from selected network devices, while NTA was used to collect and display NetFlow volumetric activity data from key layer three routers into a dedicated Microsoft® SQL Server database. The SolarWinds™ Orion Platform Core displayed the SNMP and NetFlow data graphically via a web interface. CSCI managed the DASCAN SolarWinds instance on the Secret Internet Protocol Router Network (SIPRnet) and was granted full access to the Marine Corps' SolarWinds instance on the Non-Secure Internet Protocol Network (NIPRnet) in order to collect bandwidth utilization and providing reports. The SIPRnet database was then returned to Springfield for in-depth post-event analysis.

After refining collection and analysis techniques on the two WTI networks, CSCI then documented the network activities of the much larger First Marine Expeditionary Force's (I MEF) Large Scale Exercise 2016 (LSE-16). The CBM team used the Marine Corps' own Solarwinds instances to record NIPRnet, SIPRnet, and "BlackCore" network activities and a perform a complete post-event database analysis.

THE RESULTS

Complete bandwidth usage baselines were documented and analyzed for WTI 2-16 and LSE-16. CBM's activities also revealed that the **SolarWinds suite can effectively provide network management** for USMC tactical networks, but highlighted the need for standardization and in-depth training. Beyond simply providing network device awareness, the suite can provide network transparency by tracking upper-layer application activities to visually display a near real-time usage baseline. This rolling "application baseline" provides a useful tool for tactical network managers to recognize application usage anomalies. Prompt recognition and investigation of deviations from expected baselines are critical for an effective network cyber defense.

For a full report or more information about this project, contact Jack Samar: jsamar@csci-va.com or 703-923-7640.