CASE STUDY: MOBILITY ACCESS

Prepared by: James M. Thompson, MAG Aerospace

Case Study – Mobility Access

The following case study is hypothetical and provided to illustrate a portion of the MAG Aerospace process.

Mission Objectives

A Department of Defense (DoD) command required mobility for senior military and civilian decision makers when they were outside their campus environment. Specifically, the command required that decision makers have access to the classified enclave whether the decision maker was in an area with SIPRnet access or just Internet connectivity. The requirements specified that the commander and key staff have laptops and/or tablets which could connect wirelessly or through cellular through the Internet to the secure network anywhere in the world.

Environment and the Threat

The environment which the decision makers moved through varied from having a high level of physical security to not having much physical security, i.e., within a commercial hotel.

The threat outside of controlled space was not easily managed. While the end user device (EUD) included data at rest (DAR) as well as encryption tunnels for data in transit, the main challenge was addressed using well-defined techniques, tactics, and procedures (TTPs) for the use of the mobility EUDs. These TTPs were taught prior to the EUD being issued.

The environment and threat differed for each geographically dispersed location. The threat required TTP implementations which specified when, where, and how the remote mobility package could be employed.

The decision to develop the TTPs turned out to be excellent. It allowed the command to implement management tools as well as procedures which provided the Authorizing Official for the network information on the location of each remote mobility EUDs, all the while also gaining expertise in secure wireless before expanding.

CSfC Architecture

The command had heard of the NSA's Commercial Solutions for Classified (CSfC) program and contacted MAG Aerospace for help in design, assembly, and integration of the Campus WLAN in accordance with the CSfC Mobility Access Capability Package (MACP). The command tasked MAG to take the design through to CSfC registration which included testing and providing a body of evidence to the NSA and the Authorizing Official (AO) in order to obtain an Authority to Operate (ATO) for the end user devices and the MACP gray network.

1. Mission Vulnerabilities

Moving from a secure wired environment to allow remote access provided a number of training challenges. The laptops and tablets run a registered CSfC data at rest (DAR) solution which meant they were considered Unclassified when not powered. Therefore, the devices were allowed off Campus without Secret classification labels.

End users would use these devices from hotels when traveling. Therefore the user would need techniques dealing with a hotel's 'captive portal'. This could be accomplished through a separate retransmission device or a dedicated outer VPN device.

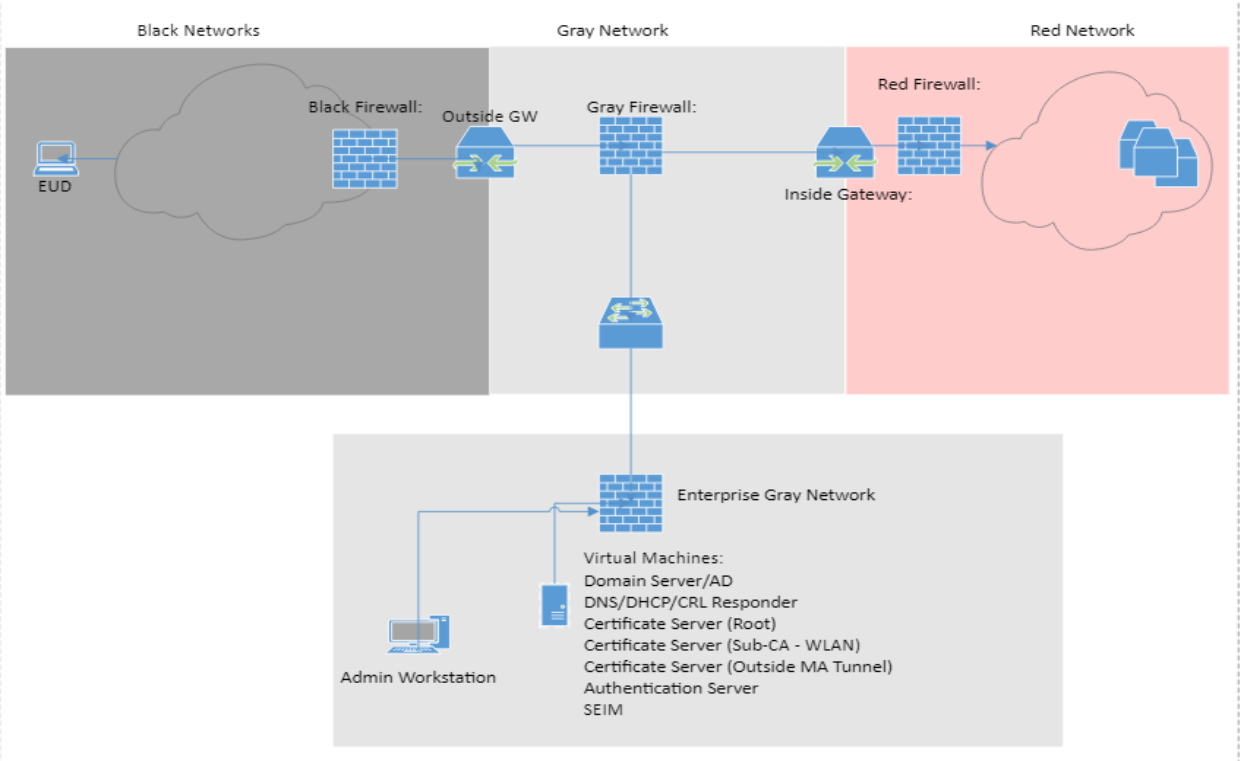
Some end users would use these devices from overseas (OCONUS) locations. This presented an issue of identifying the risk involved, mitigating the risk (which could be restricted or even no use of the MA device), and monitoring.

All of the users of the MACP attended training on the techniques, tactics, and procedures (TTPs) required for use of the devices. At the end of training, the user signed an agreement to follow the TTPs and any/all risk mitigation issues.

2. Mobility Access Design and CSfC Registration

The MAG engineers, using government-provided equipment, built a lab which emulated the eventual full implementation. This lab was then used to test the solution and fill out the CSfC checklist.

A formal test plan was developed; the solution was tested using a team of multidiscipline engineers to ensure architecture and the dual layers of cryptography to protect data in transit with completely independent separation of both hardware and software. The team confirmed each layer came from a different vendor with verification the crypto libraries were different between layers. Finally the overall package fit the basics of the CSfC's reference designs. Where there were any deviations from the CSfC's referenced design or the compliance checklist, this was documented, evaluated, and then sent as part of the overall registration process. Once these were explained, validated, and approved, the CSfC sent their registration letter to the customer's AO.



3. Mobile Access Survey

As part of the overall validated mobile access design, MAG performed a mobile access and datacenter survey to identify rack space and placement of equipment in the customer's datacenter. The survey was completed with CSfC MACP specifications in mind to provide the customer an understanding of risk and overall security. The survey also identified tactics, techniques, and procedures required for end users and system and network administrators for operations and use of the mobile devices.

4. Implementation

The customer contacted the governing authorities to allow mobile access to the secure network from remote locations. This was by no means a small hurdle, and MAG provided the customer with a System Security Architecture document which showed the multiple levels of protection in depth for implementing the MACP infrastructure and end user devices.

The MAG development engineers worked closely with the production networking, system administrator, and cybersecurity teams. One of the concerns that production had was the number of man-hours the mobile access support would take away from the current effort to maintain the network. There was very little slack in their support budget. The MAG engineers provided a MTBF/MTTR study along with a capacity planning guide which identified the number of hours needed for a number of critical tasks in networking, help desk, system administration, PKI administration, and cybersecurity. The MAG team then worked with the director of the production network to draft a manpower document to support mobile access within the command.

The MAG engineers went through the re-registration of the Mobile Access and registration of Data at Rest during the implementation period. This allowed the registration and implementation to flow directly into production without lapse in the ATO.

5. Mission Success

Initially the mobile access users came from the communications group, both development and production, as part of test and evaluation. This took less than three months before mobile devices were provided to the commander and other senior decision makers. However, this short time period for evaluation was essential to the overall success of the program. The communications personnel found issues, solved problems, and improved the overall design before the commander received his device.