CASE STUDY: CAMPUS WLAN

Prepared by: James M. Thompson, MAG Aerospace

Case Study – Campus WLAN

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 needed mobility for senior military and civilian decision makers throughout their campus environment. The command sought secure campus wireless for their classified enclave throughout meeting rooms in more than a dozen buildings on their main campus and throughout their geographically dispersed campus. Specifically, they were interested in the commander and key staff having laptops and tablets which could connect wirelessly to the secure network.

Environment and the Threat

The campus environment at the headquarters (HQ) has a high level of physical security as well as a larger standoff distance from the fence to the buildings. These essentially windowless buildings help prevent the wireless signal from extending out beyond the campus-controlled area.

Additionally, the HQ campus is a U.S. military base which provides restricted access and physical security outside the HQ boundaries.

This campus environment and the threat would be different for many of the geographically dispersed locations. This would make that implementation more difficult, so the plan was modified to limit the initial secure wireless implementation to the HQ campus then address each of the other locations as the implementation was expanded. This decision turned out to be excellent, allowing the command to work out a number of techniques, processes, and procedures 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 Campus WLAN Capability Package (CP). 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 wireless network.

Mission Vulnerabilities

Moving from a secure wired environment to wireless provided a number of training challenges. The initial laptops and tablets, while not running an approved data at rest (DAR), prevented them from being used off campus. They were marked with Secret classification labels. While this was addressed in future iterations as the campus WLAN expanded to other geographically dispersed locations, it did present the opportunity to develop a training program for wireless users.

Wireless Network Design and CSfC Registration

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

The solution was tested to ensure that there were two layers of cryptography to protect the data in transit with completely independent separation of both hardware and software. Each layer was from a different vendor with verification that the crypto libraries were different between layers. Finally the

overall package fit the basics of the CSfC's reference designs. However, there were some deviations from the CSfC's design which were documented then sent up as part of the overall approval process. Once these were validated by the CSfC, MAG, and the customer, the CSfC sent their registration letter to the customer's AO.

Site Survey

With a validated secure wireless design, MAG performed the site survey to identify the placement of each access point in multiple buildings on the HQ campus. The survey was done with 802.11ac specifications in mind to provide the customer with the highest bandwidth possible. The survey also went to the fence line to ensure that the signal was not strong enough to enable hacking outside the physical fence.

Implementation

The customer contacted the governing authorities to allow wireless within the buildings prior to the installation of access points. 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 the secure wireless network. This document was pivotal in getting approval.

The MAG development engineers worked closely with the production networking team and cybersecurity. One concern that production had was the number of man-hours the wireless would take away from the current effort to maintain the network. There was very little slack in their budget. MAG provided a manpower study based on the Mean Time Between Failure/Mean Time To Repair (MTBF/MTTR) wireless systems equipment 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 wireless within the command.

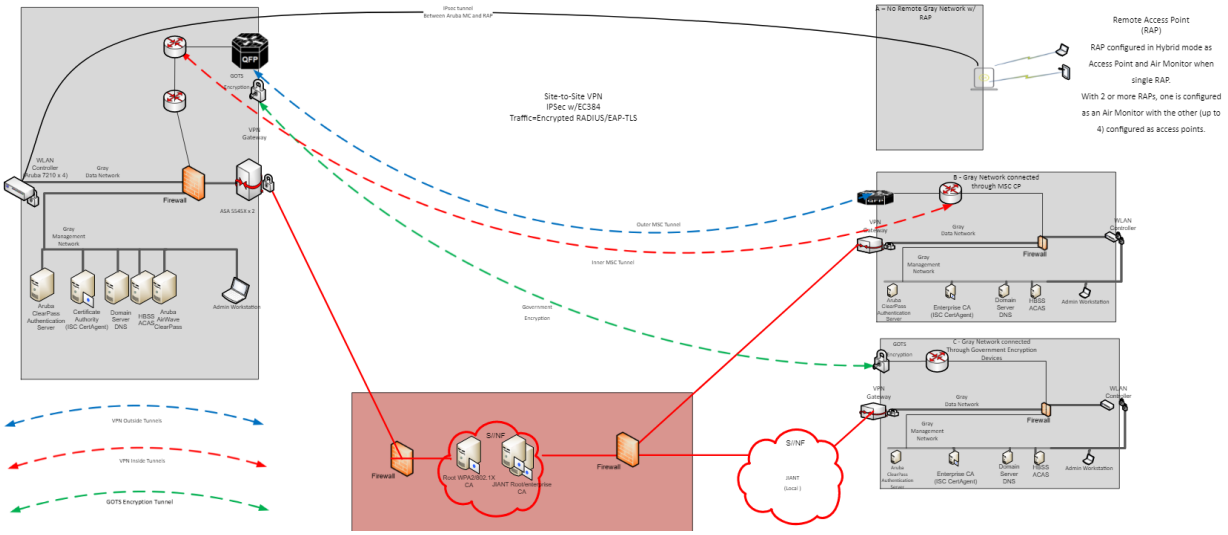
The MAG engineers went through the re-registration of the campus wireless and registration of Data at Rest during the implementation period. This allowed implementation to flow directly into production without a lapse in the ATO.

Mission Success

Initially the wireless users came from the communications group, both development and production. In less than six months, wireless laptops were provided to the commander and other senior decision makers. This short time period was essential to the overall success of the program. The communications personnel found issues, solved several problems, and improved the overall design before the commander received his machine.

The command and MAG have registered the campus WLAN twice since implementation. The number of users has grown to approximately 1000 which includes not only the senior decision makers but also many others who have found greater efficiency through mobility using the campus wireless. The issue with a geographically diverse campus has been solved for multiple locations so that personnel can move between the areas and connect easily to the network wirelessly. This same extended campus capability is used for some aircraft operations and is being looked at for some tactical initiatives.

Additional Network Design Information



The Client End User Devices (EUDs) include laptops and tablets. The client connects using WPS2-Enterprise through an Aruba Controller and Aruba Radius server for authentication. Once this connection is made, the EUD is connected to the wireless 'gray' network (outer tunnel) with the ability to connect to only a single location/device, the VPN gateway. The client then brings up their VPN which creates the inner tunnel to the Red network. The certificate being used for the outer tunnel is an RSA-4096 SHA-384 while the inner tunnel uses an Elliptical Curve (P-384) certificate. Both tunnels are encrypted using AES with the outer tunnel (WPA-2-Enterprise) being AES-128 which the inner tunnel uses AES-256 (IPSec IKEv2) and is fully CNSA compliant.

The VPN gateway is a Cisco ASA which provides the vendor diversity required in the CSfC checklist. This vendor diversity ensures that the crypto libraries are different between the two tunnels. The connection to the geographically separate portions of the campus currently use GOTS Type-1 encryption devices with some consideration in using a CSfC MSC CP to connect the gray networks.